2

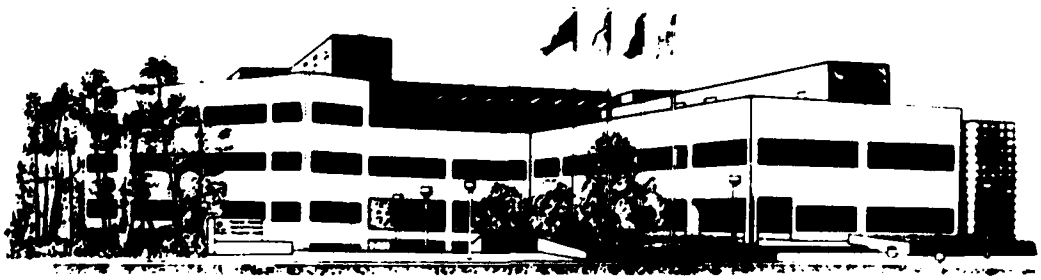
U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# DIGITAL SYSTEMS VALIDATION HANDBOOK-VOLUME II

DIGITAL SYSTEMS VALIDATION
FAA TECHNICAL CENTER

FEBRUARY 1989



FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER

## NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

**Technical Report Documentation Page**

1. Report No.
DOT/FAA/CT-88/10

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
DIGITAL SYSTEMS VALIDATION HANDBOOK - VOLUME II

5. Report Date
FEBRUARY 1989

6. Performing Organization Code
CRMI

7. Author(s)
SEE TABLE OF CONTENTS

8. Performing Organization Report No.
DOT/FAA/CT-88/10

9. Performing Organization Name and Address
COMPUTER RESOURCE MANAGEMENT INCORPORATED
950 HERNDON PARKWAY SUITE 360
HERNDON, VA 22070

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTFA03-86-C-00042

12. Sponsoring Agency Name and Address
U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NJ 08405

13. Type of Report and Period Covered
HANDBOOK

14. Sponsoring Agency Code
ACD-230

15. Supplementary Notes
Point of Contact: Pete Saraceni, ACD-230
FAA Technical Center
Atlantic City International Airport, NJ 08405

16. Abstract

Volume II covers detailed technical topics such as latent faults; data buses; integrated assurance assessment; analytical sensor redundancy; and protection against lightning, electromagnetic interference, and high energy radio frequency fields. These topics are covered in detail to familiarize the certification engineer with the issues involved in implementing the new technologies.

Volume II covers topics that will enable the certification engineer to understand the information presented in type certification and supplemental type certification documentation, to understand variations in the implementation of technologies, and to discuss them with the design engineer.

Volume II also addresses some of the soon-to-be-available technologies in the "Advanced Validation Issues" chapter. The direction of aviation research in the United States is discussed along with challenges and problems that confront the certification engineer in certifying the new technologies.

Since the topics discussed in this Handbook are at the forefront of technological research, some of the concepts presented are subject to discussion by experts in the field. In these areas, the Handbook presents various viewpoints alerting the certification engineer to the various views so that this information will be considered in formulating decisions and developing certification criteria.

17. Key Words
Avionics, Digital, Validation, Certification, Reliability, Redundancy, Latent Faults, Fault Insertion, Data Buses, Lightning, Radio Frequency Fields, Transients, Verification, Composites, Modeling

18. Distribution Statement
This document is available to the U.S. public through the National Technical Information Service, Springfield, Virginia 22161

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No. of Pages
900

22. Price

Reproduction of completed page authorized

# DIGITAL SYSTEMS VALIDATION HANDBOOK - VOLUME II

## TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

# LIST OF AUTHORS

Clifton A. Clarke
Boeing Commercial Airplane Company
P. O. Box 3707
Seattle, WA 98124

William W. Cooley
Science & Engineering Associates, Inc.
701 Dexter Avenue
Seattle, Washington 98109

Hardy P. Curd
Computer Resource Management, Incorporated
950 Herndon Parkway
Herndon, VA 22070

Donald Eldredge
Battelle Columbus Division
505 King Avenue
Columbus, OH 43201

Robert E. Evans
FAA Technical Center
Atlantic City International Airport, NJ 08405

Myron J. Hecht
SoHaR, Incorporated
8500 Wilshire Boulevard
Beverly Hills, CA 90211

William E. Larsen
FAA Field Office
P. O. Box 25
Moffett Field, CA 94035

Susan Mangold
Battelle Columbus Division
505 King Avenue
Columbus, OH 43201

Roger McConnell
CK Consultants
5473 A Clouds Rest
Mariposa, California 95338

R. L. McDowall
Computer Resource Management, Incorporated
950 Herndon Parkway
Herndon, VA 22070

John G. McGough, Consultant
150 Walnut Street
Ridgewood, NJ 07450

Barbara G. Melander
Science & Engineering Associates, Inc.
701 Dexter Avenue
Seattle, Washington 98109

Lloyd N. Popish, Consultant
525 Davenport Court
Sunnyvale, CA 94087

John E. Reed
FAA Technical Center
Atlantic City International Airport, NJ 08405

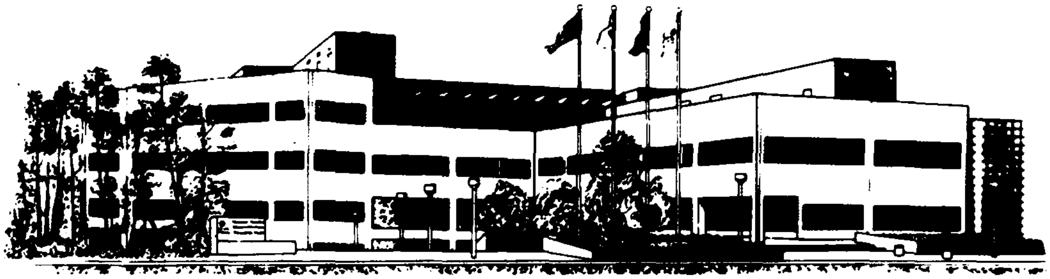
Deborah L. Shortess
Science & Engineering Associates, Inc.
701 Dexter Avenue
Seattle, Washington 98109

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II DIGITAL SYSTEMS VALIDATION

## CHAPTER 1 SUMMARY



**PREPARED BY:**

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

**PREPARED FOR:**

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# EXECUTIVE SUMMARY

The Digital Systems Validation Handbook - Volume II (DOT/FAA/CT-88/10) is a followup and companion to the Handbook - Volume I Validation of Digital Systems in Avionics and Flight Control Applications (DOT/FAA/CT-82/115).

Volume I was issued in July 1983 and revised in September 1986. It deals with system overview topics such as the System Life Cycle, Mission Factors, System Architectures, Crew Workload Evaluation, Current Validation Procedures, Recommended Validation Procedures, and Recommended Configuration Management Procedures.

The emphasis in Volume I is on the validation of digital avionic systems. Validation of a system is the determination that the system is well grounded on principles or evidence. The topics presented in Volume I assist the certification engineer in understanding how to determine if the validation of a system has been correctly performed.

The emphasis in Volume ~~II~~ is on the certification of advanced technology digital avionic systems, as well as their validation. ~~Volume II~~ covers detailed technical topics such as latent faults; data busses; integrated assurance assessment; analytical sensor redundancy; and protection against lightning, electromagnetic interference, and high energy radio frequency fields. These topics are covered in detail to familiarize the certification engineer with the issues involved in implementing the new technologies.

Volume ~~II covers~~ topics that will enable the certification engineer to understand the information presented in type certification and supplemental type certification documentation, to understand variations in the implementation of technologies, and to discuss them with the design engineer.

Volu~~me II~~ also addressed are some of the soon-to-be-available technologies in the "Advanced Validation Issues" chapter. The direction of aviation research in the United States is discussed along with challenges and problems that confront the certification engineer in certifying the new technologies.

Since the topics discussed in this Handbook are at the forefront of technological research, some of the concepts presented are subject to discussion by experts in the field. In these areas, the Handbook presents various viewpoints alerting the certification engineer to the various views so that this information will be considered in formulating decisions and developing certification criteria.

It is intended that this Handbook will be a living document. As technology advances, addenda to existing chapters will be issued. Where major new technologies are addressed, new chapters will be added to the Handbook. The Federal Aviation Administration (FAA), therefore, solicits your comments and

suggestions for the improvement of this Handbook. Please address any comments to:

Flight Safety Research Branch, ACD-230
Digital Systems Validation Handbook
FAA Technical Center, Bldg. 201
Atlantic City International Airport, New Jersey 08405

# TABLE OF CONTENTS

# 1. INTRODUCTION

## 1.1. Background

The rapid developments in computers and digital technology over the past 20 years have made digital systems increasingly useful in aircraft. As computers become more sophisticated, they are able to perform an increasing number of tasks which were previously performed by the pilot or by analog systems. As a result, certification engineers are seeing increasing numbers of digital systems proposed for inclusion in new generations of aircraft and for incorporation into existing aircraft designs.

The new systems pose a number of problems for the certification engineer. Error limits must be set for flight-critical, flight-essential, and non-essential systems. In setting error limits, safety is paramount, but other factors must also be taken into account. These factors include cost for incremental error reduction, weight penalties, and system interactions.

Integrating a new digital "black box" into an existing design changes many of the electromagnetic characteristics of the aircraft. Care must be taken to ensure not only that the black box performs its functions within the required error limits but also to ensure that its addition does not degrade any other systems which have already been certificated.

The design of a completely new aircraft poses its own problems in digital technology. Each individual component must meet error limits, weight limits, and size limits. Systems (composed of several components more or less collocated) must meet these requirements, plus the requirements of being able to collect systemic information and pass it on to other systems while not interfering with the operation of any of the other systems.

In the summer of 1975, the Federal Aviation Administration (FAA) and the National Aeronautics and Space Administration (NASA) began to consider and plan a joint program to assess and upgrade the technologies used to evaluate the reliability of digital flight control and avionics systems. In 1976, the FAA and NASA cosponsored a workshop on digital flight controls and avionics.

A number of reports emerged from this program. These reports were collected into the Digital Systems Validation Handbook - Volume I (DOT/FAA/CT-82/115) "Validation of Digital Systems in Avionics and Flight Control Applications." Since the 1976 workshop and the 1982 publication of Volume I, however, a number of technological advances have been made. It is time to review the issues of digital avionics and flight control systems in light of the new, emerging technologies.

There are approximately 20 areas of technological investigation that have been sponsored by the FAA and/or NASA. The investigations, the final technical reports, and the technical results are the basis for the tutorial materials in this Handbook.

## 1.2. Purpose

The purpose of this Handbook is to give the certification engineer background information on the emerging technologies which will figure prominently in designs now being submitted for certification and anticipated by the end of the century. Certification engineers will then be more knowledgeable in these new areas of technology so that they may more effectively evaluate the materials submitted in support of a request for a Type Certificate (TC) or Supplemental Type Certificate (STC).

This Handbook will serve as a guide to the certification engineer. Each chapter addresses a specific area of technology. Alternate viewpoints are presented as appropriate. Worked examples guide the engineer through the application of the technology. Bibliographies in each chapter give the engineer sources of additional information about the chapter topic. Each chapter can be considered a stand-alone volume about the subject area in question and can be separated into its own volume for ease of reference.

## 1.3. Scope

This Handbook provides the certification engineer with information on emerging technologies. Since much of the technology in this Handbook is new, some of it is still at issue and is subject to various interpretations. For completeness, alternate viewpoints have been included wherever appropriate. This will provide the certification engineer with the widest variety of information available from which to make certification decisions.

The user should also note that although the Handbook contains the latest information available at the time each tutorial was written, some of this information may be out of date. The certification engineer should therefore use this Handbook as a guideline rather than a hardline.

# 2. HANDBOOK ORGANIZATION

## 2.1. Handbook Format

Thıs Handbook is a dynamic document. As such, it is being issued in a loose-leaf format so that it can be expanded easily as knowledge of newer technology applications becomes available. Each chapter has the same type of tutorial/worked example format and will be updated as a function of technological progress in the areas of civil fixed or rotary wing aircraft, electronics, and system integration. As new information is received, it will be issued either in the form of chapters to be added or revision pages for existing chapters.

The Glossary and the Acronym list for the entire book contain information from all chapters.

## 2.2. Chapter Formats

Each chapter contains its own Table of Contents, List of Acronyms and Abbreviations, Glossary, and References. The individual acronym lists are particularly important when dealing with such diverse topics since different subject areas may use common acronyms with different interpretations.

## 2.3. Contents of Technical Chapters

### 2.3.1. Chapter 3 - Integrated Assurance Assessment Activities

This chapter covers Integrated Assurance Assessment methods including probability analysis, fault-tree analysis, and failure modes and effects analysis. It shows how these methods may be meshed to establish the air-worthiness of a flight-critical system. It also demonstrates how these methods reinforce each other in this determination.

### 2.3.2. Chapter 4 - Quadruplex Digital Flight Control System Assurance Assessment

Quadruplex digital flight control systems are an evolution from the dual-dual architecture, using four parallel systems rather than two redundant systems. This chapter covers the history of the technology and identifies the functional relationships between the hardware and the software.

### 2.3.3. Chapter 5 - Advanced Fault Insertion & Simulation Methods

One method of testing flight-critical systems is to insert faults into the system to see if they are found by the error detection and correction mechanisms embedded in the system. There are three categories of faults: (1) faults which are inserted and found, (2) faults which are inserted and not found, and (3) no-fault situations which are identified as faults. This chapter covers the hardware systems used in the insertion of faults and the interpretation of the results.

### 2.3.4. Chapter 6 - Data Bus Integrity Issues

Data buses are currently used in flight control and avionics applications to transfer data. Errors in data transmission may result in erroneous or incomprehensible data being transmitted to processors or to flight control mechanisms. This chapter covers the integrity of data buses. It contains an overview of alternative data bus architectures, including, an evaluation of their reliability. It also addresses areas of uncertainty in reliability and minimum currently accepted redundancy standards.

### 2.3.5. Chapter 7 - Analytical Sensor Redundancy

Analytical sensor redundancy is the use of software algorithms to substitute for hardware in providing redundant signals. If an accurate model of the airframe can be created, the software can extrapolate from prior observations and make short-term predictions about the status of the aircraft. This allows the system to compensate for hardware failure. This chapter covers the details of analytical sensor redundancy, its uses, and its limitations.

### 2.3.6. Chapter 8 - Software Reliability Assessment Methods

As flight functions are increasingly carried out by digital systems, the issue of the reliability of the software controlling these systems becomes more and more important to flight safety. Higher order languages, testing, debugging, and software engineering can all contribute to increased reliability. Models have been developed to assess the reliability of these systems. This chapter covers existing software reliability assessment models. It compares the models and gives an overview of their reliability as predictive tools.

### 2.3.7. Chapter 9 - Software Fault Tolerance

This chapter covers software methods and techniques used for detection and correction of faults. These may include checks on the reasonableness of data and comparison of information from redundant systems. This chapter also covers fault tolerant design using complexity measures and other techniques.

### 2.3.8. Chapter 10 - Latent Faults

Latent faults are faults which have occurred, but have not been detected because the path on which they have occurred has not been traveled. They can be both hardwaie and software faults. This chapter covers experiments conducted to inject faults and discover them. It discusses the prediction, triggering, identification, and correction of latent faults.

### 2.3.9. Chapter 11 - Guidelines To Assess EMC Designs

This chapter covers guidelines that may be used to assure electromagnetic compatibility during the design process. It also includes information on how the certification engineer can assess how well a design or system adheres to the guidelines.

### 2.3.10. Chapter 12 - Fast Rise Time EMC Transient Testing

This chapter discusses EMC transient testing experiments. Presently, the chapter contains the theory for the testing only, since the testing itself has not been conducted and may not be completed in time for this handbook.

### 2.3.11. Chapter 13 - Lightning Studies

As more and more flight-critical systems are digitized and as composite materials become more widely used in aircraft construction, the threat from lightning increases. This chapter covers currently accepted information about lightning including estimates of currents, electric fields, and magnetic fields which aircraft might expect to encounter. It reviews methods for protecting electrical and electronic equipment from this hazard and it covers methods for isolating equipment so that potential damage may be limited.

### 2.3.12. Chapter 14 - High Energy Radio Frequency Fields

With changes in aircraft construction from aluminum to composites and increased criticality of software-based digital flight control and avionic systems, total aircraft RF susceptibility hardening and protection is vital. This chapter assesses the present criteria, specifications, and procedures for industry and certification authorities in the light of increasing levels of RF over a wide frequency range.

### 2.3.13. Chapter 15 - Electromechanical Actuator Systems (EMAS)

This chapter will cover the technical description, testing, and redundancy requirements for smart servos and actuators, primary and secondary power sources, and digital engine controllers.

### 2.3.14. Chapter 16 - Advanced Validation Issues

This chapter gives a brief overview of areas where advances are likely in the near future. As new information becomes available, each of these sections may be expanded to form a separate chapter.

The topics to be covered are:

- Artificial Intelligence
- Remote Processing
- Robotics (Testing Control)
- Advanced Architecture (Distributed Fault Tolerant Processing)
- Advanced Controls and Displays

- Voice Command Processing
- System Integration Technology

# ACRONYMS AND ABBREVIATIONS

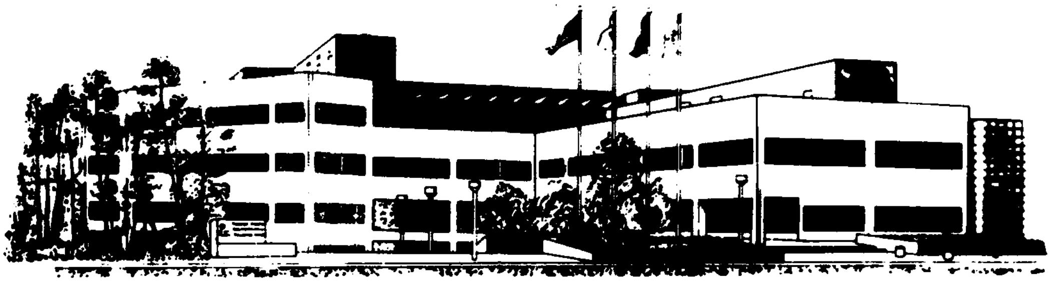
| | |
|---|---|
| CRMI | Computer Resource Management, Incorporated |
| CT | Technical Center Identification code |
| DOT | Department of Transportation |
| EMAS | Electromechanical Actuator System |
| FAA | Federal Aviation Administration |
| NASA | National Aeronautics and Space Administration |
| RTCA | Radio Technical Commission for Aeronautics |
| SAE | Society of Automotive Engineers |
| STC | Supplemental Type Certification |
| TC | Type Certification |

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 3
## INTEGRATED ASSURANCE ASSESSMENT



**PREPARED BY:**

**COMPUTER RESOURCE MANAGEMENT, INC.**
**950 HERNDON PARKWAY, SUITE 360**
**HERNDON, VIRGINIA 22070**

**PREPARED FOR:**

**FEDERAL AVIATION ADMINISTRATION**
**TECHNICAL CENTER**
**ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405**

## NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

Section Page

APPENDICES

# LIST OF ILLUSTRATIONS

## LIST OF ILLUSTRATIONS (Continued)

## LIST OF TABLES

# 1. INTRODUCTION TO INTEGRATED ASSURANCE ASSESSMENT

## 1.1. Justification for Integrated Assurance Assessment

The validation of flight-essential and flight-critical digital systems is of crucial importance in the determination of each system's airworthiness. This tutorial is a reference for certification engineers involved in the functional assessment of aircraft which use digital systems for avionics and flight control functions. Part 25 of the Federal Acquisition Regulation (FAR) (specifically FAR 25.1309) contains the requirements for flight-essential and flight-critical avionic systems. Federal Aviation Administration (FAA) Advisory Circular (AC) 25.1309-1 provides guidance material for demonstrating compliance with FAR 25.1309. This AC outlines the use of quantitative safety analysis techniques that may include: (1) Probability Analysis, (2) Fault Tree Analysis, (3) Failure Modes and Effects Analysis (FMEA), and (4) other comparable techniques for determining compliance with the requirements of FAR 25.1309 (b).

The use of any of these analysis techniques in isolation for an entire avionic system introduces some difficulties. To eliminate or minimize these difficulties, an Integrated Assurance Assessment (IAA) is desirable. A model for an integrated assurance approach may include a number of techniques, each contributing to the value of the analysis. For instance, fault tree analysis provides assurances that most system components have no single failure mode that results in system failure. When components have several failure modes that may have different effects on system readiness, fault tree analysis may prove cumbersome and inefficient. In this latter case, FMEA may be used to extend the examination below the component level to the failure modes of the individual piece-parts that comprise the component. Integrating fault tree analysis and FMEA permits the diagnosis of system failure from system-level functions through Integrated Circuit (IC) pins.

The above simple integration may be used to develop a probability for system failure. If the analysis contains no errors, this probability is true. If an error exists, the probability may be erroneously low and go undetected. Computation of the system failure probability by an independent analytical technique would either confirm the results of the above analysis or detect that an error was made. A computer-aided reliability analysis would provide that independent confirmation. Extending the integration to incorporate this technique means that the scope of the analysis begins at the system level and extends through the piece-part level, a system probability error may be computed, and a confirmation of that system probability error obtained.

In performing the fault tree analysis or FMEA, the effects of certain faults may not be known or may be uncertain. If this is the case, a technique for determining or verifying the effects of certain faults would improve the IAA. Fault Insertion is a technique for determining or confirming the fault effect.

Incorporating the fault insertion technique in an integrated assurance model improves the analysis that may be performed with that model.

The IAA model defined above utilizes four analysis techniques. Each of the four was incorporated in the model for specific reasons. Table 1.1-1 shows the techniques and the simplified capabilities each adds to the integrated model. Section 2 will discuss this model in greater detail.

TABLE 1.1-1. INTEGRATED ASSURANCE ASSESSMENT MODEL

| Technique | System Level Capability |
|---|---|
| Fault Tree | Determine System Failure Effect of Component and Piece-Parts; Compute System Probability of Failure |
| Failure Mode and Effect | Determine System Failure Effect of Piece-Parts |
| Reliability Analysis | Confirms System Probability of Failure |
| Fault Insertion | Confirms System Failure Effect of Component and Piece-Parts |

The evolution of an integrated assurance model is dependent on the system to be diagnosed. Simply, the capabilities of analysis, detection, annunciation, and confirmation must be provided. The specific analytic techniques that provide these capabilities may vary from model to model.

## 1.2. Primary Source for this Tutorial

The primary source for this tutorial is report Number DOT/FAA/CT-82/154, developed by the Lockheed-Georgia Company, entitled "IAA of a Reconfigurable Digital Flight Control System." The report documents an assurance assessment of a representative contemporary Digital Flight Control System (DFCS). The complementary use of various analytical techniques for safety analysis was stressed. Their primary objective was to explore and demonstrate the integrated application of reliability, failure effects, and system simulator methods in establishing the airworthiness of a flight-critical DFCS. The emphasis was on the mutual reinforcement of the methods.

## 1.3. How to Use this Document

This tutorial is divided into nine major sections:

- Section 1, "Introduction to IAA," provides an overview of IAA. It covers the Regulations and ACs to which IAA is a response. It shows four typical safety analysis techniques meshed to form an IAA model. The justification for incorporating each of the techniques is given.

- Section 2, "IAA of a Reconfigurable Digital Flight Control System," provides a discussion of the research effort introduced in Section 1. The digital system is defined and the dual-dual attribute of this system is discussed. Both the production configuration and the simulator for the subject digital system are discussed.

- Section 3, "Considerations in the Development of an IAA Model," discusses the benefits that accrue to the IAA effort for each of the safety analysis techniques incorporated. The IAA model demonstrated here was the model actually used in the subject study.

- Section 4, "Fault Tree Analysis," demonstrates the use of fault tree analysis as a top-down, deductive analysis tool to be used in the identification of conditions and functional failures that contribute to higher level component or system failure. This section contains a detailed application of fault tree analysis in the subject study.

- Section 5, "Failure Mode and Effect Analysis," demonstrates the use of FMEA as a bottom-up, inductive analysis tool to be used to determine what happens to the system or higher level components when individual parts fail. This section contains a detailed analysis of three modules of a microprocessor.

- Section 6, "Fault Insertion," demonstrates the use of fault insertion in determining and confirming fault effects by fault simulation. A detailed example is given.

- Section 7, "Failure Rate Development," demonstrates how failure rates required by the fault tree analysis and the reliability prediction tool were obtained. It does not illustrate a safety analysis technique applied in the IAA.

- Section 8, "Reliability Prediction using (Computer-Aided Redundant System Reliability Analysis) CARSRA," demonstrates the use of an analytical reliability prediction program in obtaining the probability of system failure. The details of the application of this tool to the subject study are given.

- Section 9, "Summary Statement," summarizes the tutorial. Summary commentary is given on the experience gained from performing the Redundant Digital Flight Control Analysis - relating benefits, limitations, and suggested improvements.

If the reader is interested in general knowledge, sections 1, 2, and 9 will suffice. This will provide an overview of what IAA is, when its use should be considered, and what advantages or disadvantages are likely to result from its use. Section 3 contains a detailed discussion on why the selected techniques were incorporated in the IAA model. Sections 4 through 8 contain a detailed discussion on each of the selected safety analysis techniques and their use in the subject study.

# 2. IAA OF A RECONFIGURABLE DIGITAL FLIGHT CONTROL SYSTEM

## 2.1. The Redundant Digital Flight Control System

Under report number DOT/FAA/CT-82/154, entitled "IAA of a Reconfigurable Digital Flight Control System," referenced in section 1.2, an IAA was performed on the Redundant Digital Flight Control System (RDFCS). This digital system was procured jointly by the FAA and the NASA-Ames Research Center and was a central part of the DFCS Verification Laboratory at NASA-Ames. Appendix A contains a summary description of the system architecture. While the sensors and servos are described in the production configuration, they were not actually present in the RDFCS configuration but were simulated.

In most operational modes, the system is fail-passive with a dual channel configuration. For automatic landings under Category IIIa conditions (see AC 120-28C), the system can be brought into a dual-dual fail-operational, fail-passive configuration. The classification dual-dual relates primarily to the four computer channels in the system. Each of the two Flight Control Computers (FCCs) has two channels which run frame-synchronously; each channel drives one coil of a dual-coil servo in each axis. Any indication of disagreement between the two channels in an FCC causes the servo connected to that FCC to disengage. Figure 2.1-1 summarizes the dual-dual configuration.

The RDFCS simulator is comprised primarily of a PDP 11/60 computer and the RDFCS pallet. The pallet is shown in figure 2.1-2. The PDP 11/60 computer hosts a discrete-state model of the airplane in which the RDFCS is installed. The RDFCS pallet contains the FCCs, the core memory for the FCCs, and the following devices:

- Modular Digital Interface Control Unit (MDICU) controls interface to the PDP 11/60.

- Computer Breakout Panel permits optional interruption of signals passing from MDICU to the FCC. The lower portion of figure 2.1-3 shows part of the Computer Breakout Panel.

- CAPS (Computer Aided Production Simulator) Test Adapters (CTA) permits address monitoring on the FCC processor bus. The upper portion of figure 2.1-3 shows the CTA.

- Servo Simulation Panel (SSP) simulates the dynamics of servos. The SSP is shown in figure 2.1-4.

- Discrete Switch Panel (DSP) contains switches affecting the Instrument Landing Systems (ILS). The DSP is shown in figure 2.1-5.

Appendix B contains a detailed description of the RDFCS simulator.

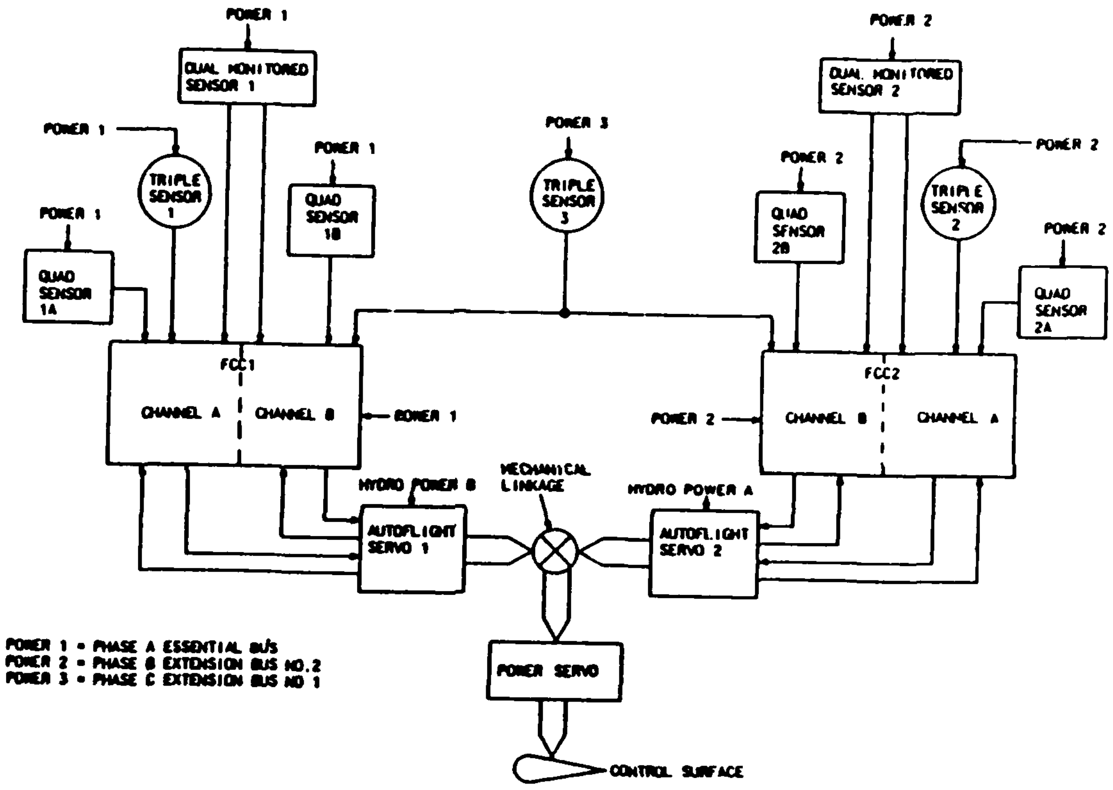


FIGURE 2.1-1. RDFCS DUAL-DUAL CONFIGURATION

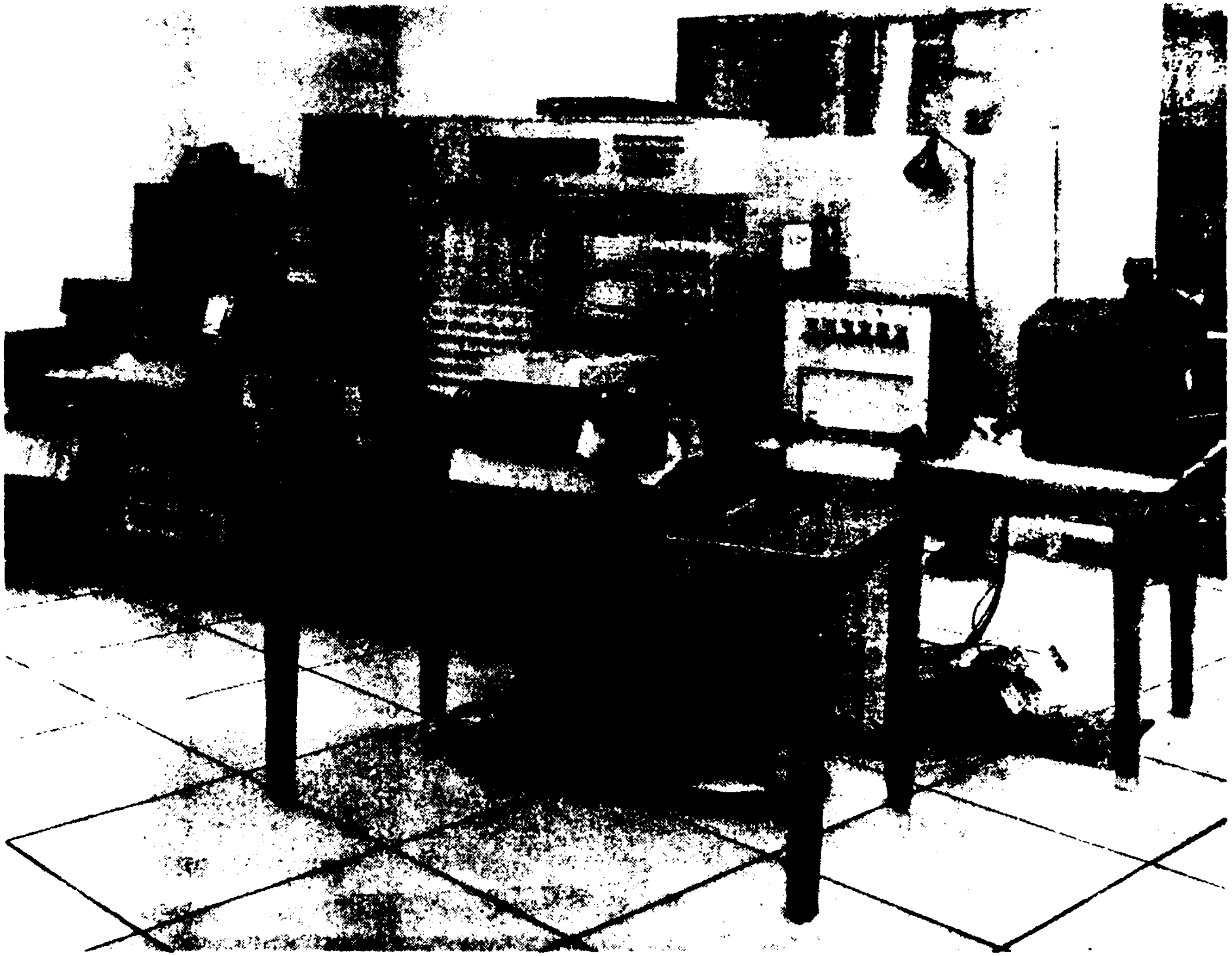


FIGURE 2.1-2. RDFCS SIMULATOR

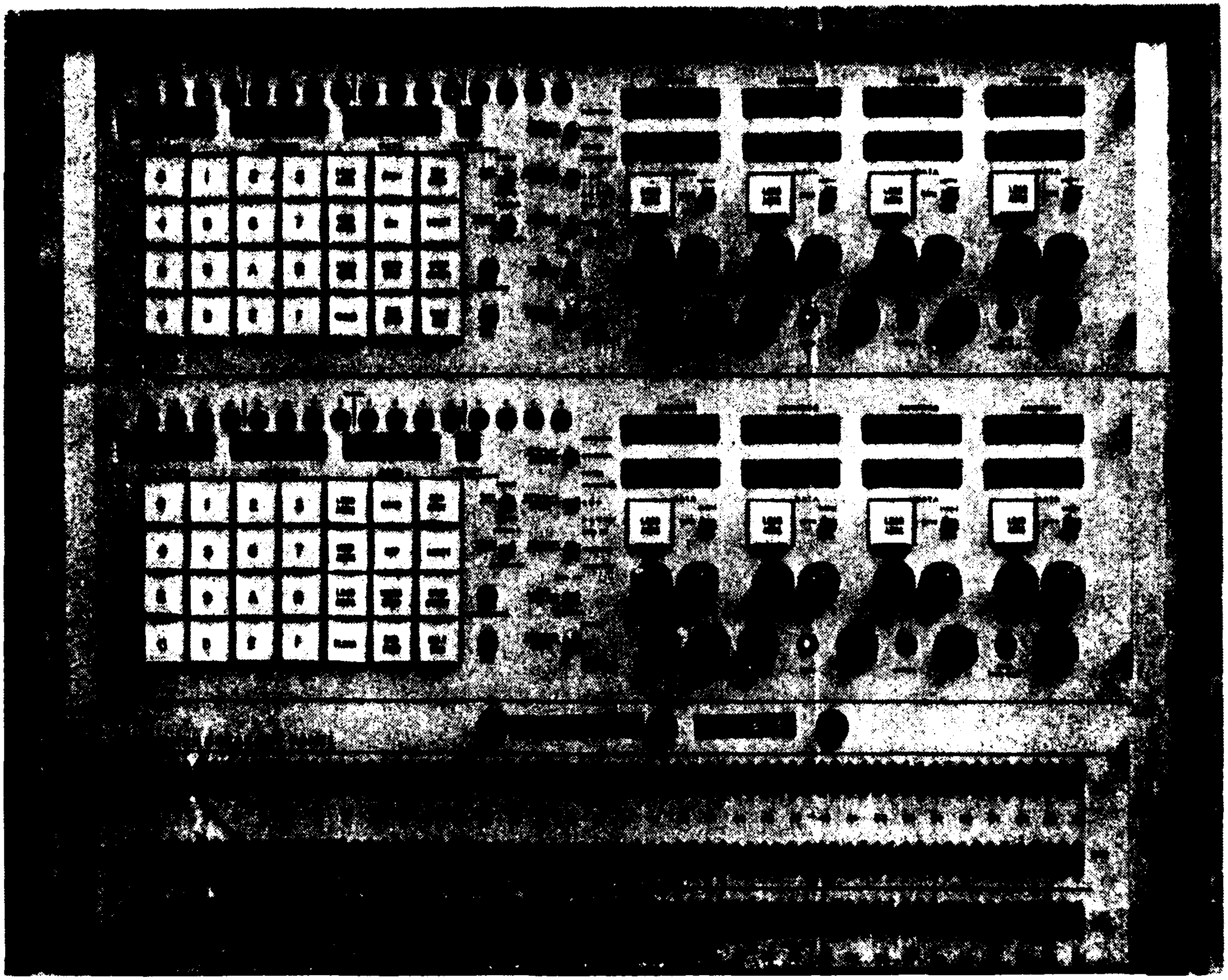


FIGURE 2.1-3. CTA AND COMPUTER BREAKOUT PANEL

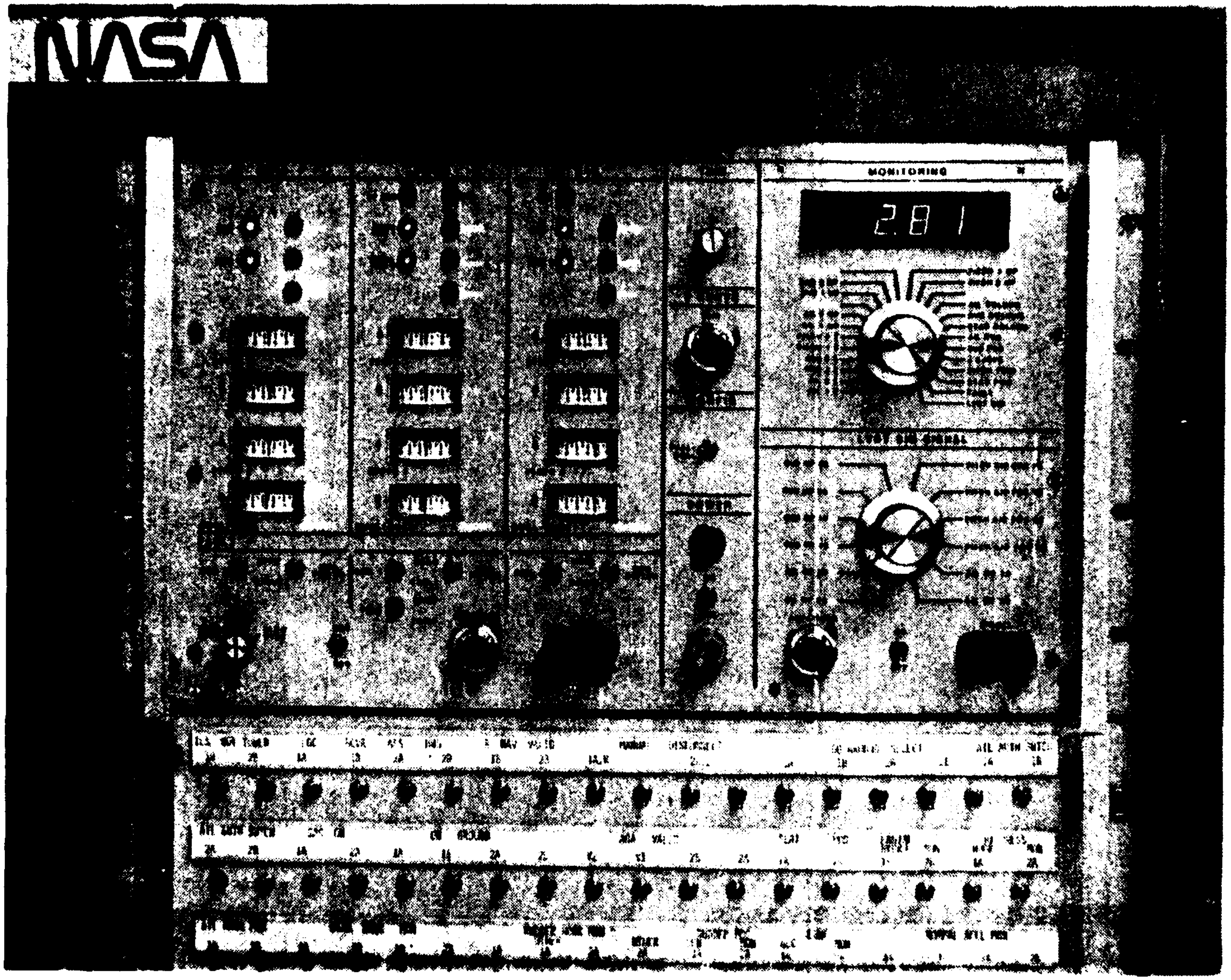


FIGURE 2.1-4. SERVO SIMULATOR PANEL

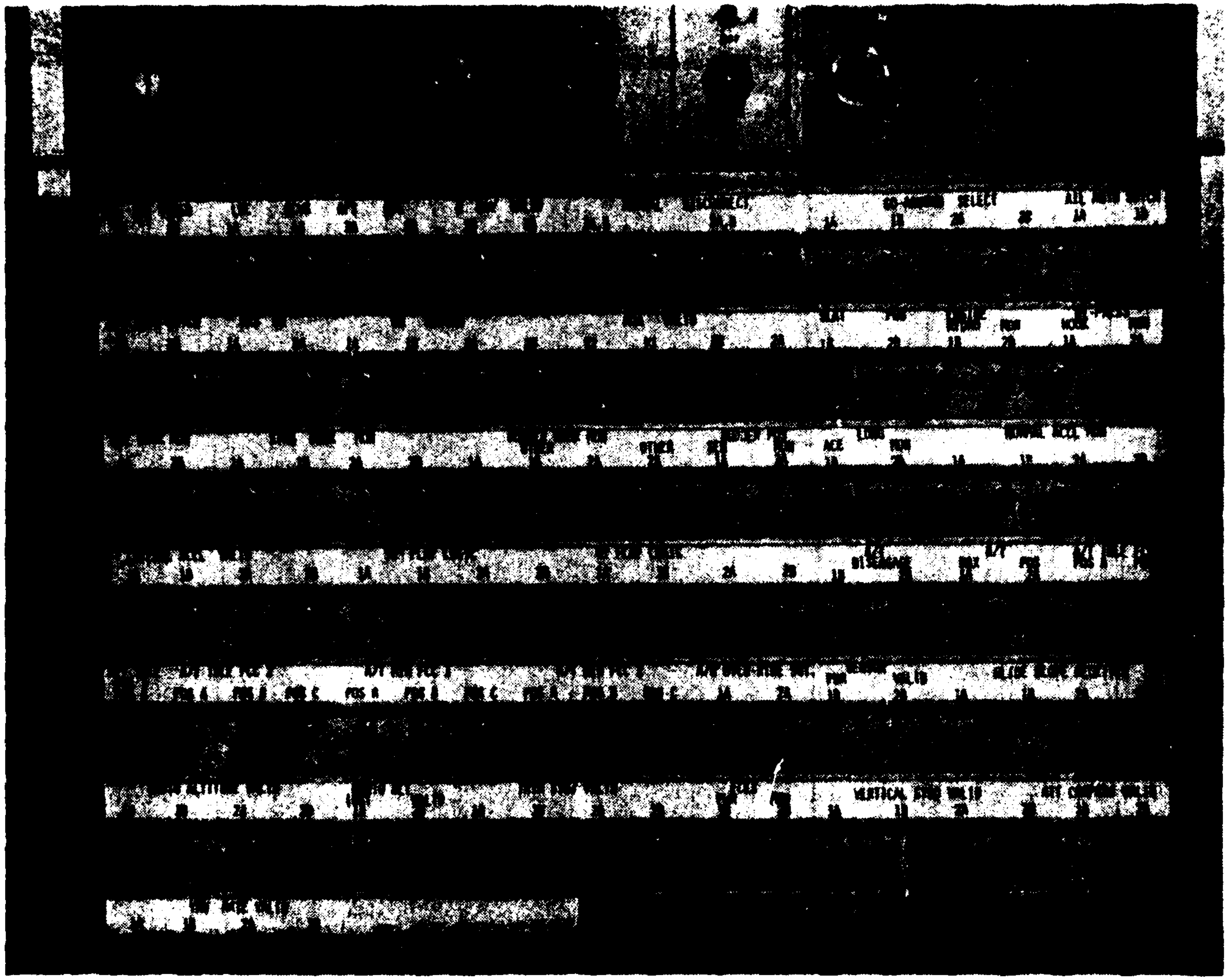


FIGURE 2.1-5. DISCRETE SWITCH PANEL

## 2.2. The IAA Study

During this study, the assurance methods of fault tree analysis, automated reliability prediction, FMEA, and fault insertion were applied to create a workable approach to confirming the airworthiness of the RDFCS. The scope of the effort was primarily limited to assessment of the automatic landing maneuver under Category IIIa conditions as defined in AC 120-28C. The analysis is based on the event that the airplane has an unacceptable deviation from the desired flight profile during the last 150 feet of descent while executing an automatic landing. This portion of the flight is the only flight phase during which the RDFCS performs a critical function. Category IIIa conditions imply that the human pilot cannot complete the landing using visual cues should the RDFCS fail. The application of safety analysis techniques was on a selective basis and addressed those system aspects identified in table 2.2-1.

The assessment consisted of the following major tasks:

- Application of fault tree analysis starting at the highest system functional level and proceeding to the hardware circuit card level and the module level for the processors.

- Development of a representative set of failure rates for the relevant hardware items.

- Application of an automated program, CARSRA, to the system failure modes affecting airworthiness.

- Application of FMEA to IC pin faults of three processor modules.

- Definition of faults to be inserted in the RDFCS. Faults to be inserted include faults used to determine the effect of the fault when analysis was not feasible, and faults used to confirm the manual analysis. These faults were subsequently inserted and the effects recorded.

## 2.3. Conclusions and Observations

The conclusions and observations resulting from this study are as follows:

- The integrated approach used in the study is capable, with diligent application, of establishing the airworthiness of a DFCS within the context of AC 25.1309-1. Specifically, this approach addresses those system aspects shown in table 2.2-1, including freedom from single-point failure modes and system failure probability.

- The IAA used in this study should be considered for use in validating other digital systems, including DFCS, in compliance with AC 25.1309-1.

## TABLE 2.2-1. ASSURANCE METHOD FUNCTIONS

|  | ASSURANCE METHOD |  |
|---|---|---|
| SYSTEM ASPECT | PRIMARY | CONFIRMATION |
| FAILURE EFFECTS |  |  |
| - COMPONENT | FAULT TREE ANALYSIS | FAULT INSERTION |
| - DIGITAL MODULE | FAULT TREE ANALYSIS, FAILURE MODE AND EFFECT ANALYSIS | FAULT INSERTION |
| - DIGITAL INTEGRATED CIRCUIT | FAILURE MODE AND EFFECT ANALYSIS | FAULT INSERTION |
| - UNTRACTABLE CASES | FAULT INSERTION |  |
| FAULT DETECTION/ ANNUNCIATION | FAULT TREE ANALYSIS | FAULT INSERTION |
| SOFTWARE FUNCTION IMPLEMENTATION | SOFTWARE TEST PROGRAM | FAULT TREE ANALYSIS |
| NO SINGLE-POINT FAILURE MODES | ABOVE, AS RELEVANT | ABOVE, AS RELEVANT |
| SYSTEM FAILURE PROBABILITY | RELIABILITY PREDICTION PROGRAM | FAULT TREE ANALYSIS<br>QUANTITATIVE EVALUATION |

- The quantitative assessment of system failure probability by two methods (fault tree analysis and analytical reliability prediction) offers increased assurance that the system meets the quantitative requirements of AC 25.1309-1. For a flight-critical system, this requirement is that the system failure probability not exceed $10^{-9}$ per hour of flight for each critical function the system performs.

- Fault insertion confirms that the fault detection capability and the fault tolerance capability described in the system documentation are actually implemented in the system. Since the fault tree analysis is based largely on the system response to faults as described in the system documentation, the fault insertion confirms that the fault tree analysis correctly reflects the behavior of the actual system in the presence of faults.

- The fault tree analysis generates software test requirements in terms of functions which the software must perform. These, in turn, provide a check of function criticality and of test requirements generated in accordance with Radio Technical Commission for Aeronautics (RTCA) Document DO-178.

- Fault tree analysis proved unwieldy below the circuit card level, because at lower levels many more functions are being performed than there are hardware failure modes. FMEA was accomplished successfully at the IC pin level.

- As a training facility and a Reconfigurable Test Bed, the RDFCS facility has significant and valuable capabilities for investigating assurance issues of currently definable DFCS architectures. It also has potential enhanced capability in certain areas, such as automated insertion of pin-level faults, for confirmation of analytically determined failure effects.

- The comparison of the time or cost required for the integrated approach reported here with that required for other possible assurance approaches was not specifically addressed in this study. However, the time required for the integrated approach is expected to compare favorably with that for other approaches, assuming the same depth of analysis. The cost should also compare favorably, provided a facility suitable for fault insertion is available.

# 3. CONSIDERATIONS IN THE DEVELOPMENT OF AN IAA APPROACH

## 3.1. General Comments

As a first step, a preliminary hazard analysis should be performed on the aircraft model. This analysis should identify those system functions that are critical and the aircraft systems that must operate correctly in order for the function to be performed correctly. According to AC 25.1309-1, a critical function is one "whose failure would contribute to or cause a failure condition which would prevent the continued safe flight and landing" of the aircraft. Essential system functions should also be identified. Essential functions are those "whose failure would contribute to or cause a failure condition which would significantly impact the safety of the airplane or the ability of the flight crew to cope with adverse operating conditions." A complete quantitative system analysis is normally required for critical systems but is more discretionary for essential systems. The following list illustrates the types of functions that may be critical:

- The primary flight control system.
- Hydraulic power for airplanes with powered flight control systems and no manual reversion.
- Secondary flight control systems, if failure of these systems can result in uncontrolled flight.
- Engine control system elements that affect all engines simultaneously.

Since the RDFCS performs critical system functions, a rigorous assurance assessment is justified. AC 25.1309-1 suggests that failure conditions for critical system functions be improbable. This requires a failure probability of less than 1.0 x $10^{-9}$. An IAA incorporating both quantitative and qualitative analyses offers advantages over the application of a single methodology. The analytical techniques used here to perform the integrated assessment are in harmony with AC 25.1309-1.

## 3.2. An IAA Approach

The steps required in performing a typical integrated assessment of the RDFCS are as follows:

- System Description: Define a baseline configuration of the RDFCS and prepare a corresponding analytical description. This description may include those additional components, beyond the RDFCS, whose exclusion would make the analysis unrealistic.

- Fault Tree Analysis: Perform a fault tree analysis beginning at the system level. To be meaningful, this analysis should extend beyond the component level to the piece-part level. This will be the case when digital modules are present with a large number of different failure modes. To perform this total analysis, both the fault tree and the FMEA tools should be used.

- Failure Rate Generation: Develop a set of representative failure rates for the components and parts of the RDFCS that will permit the evaluation of the fault tree for failure probability.

- Fault Simulation Review: Define the simulated fault conditions that are to be inserted into the RDFCS simulator. These faults shall be inserted for two purposes: to confirm the assumptions underlying the fault tree analysis, and to resolve uncertainty of the effect of the fault when analysis is not easily controlled.

- Flight Case Review: Review those flight cases available on the RDFCS simulator. If they are inadequate, augment them. Assure that all needed transitions between cases are possible.

- Reliability Analysis: Determine the tool to be used for analytic computation of system reliability. The CARSRA reliability program was used in the subject study, and is discussed in this tutorial.

### 3.3. Fault Tree Role in Integrated Assurance

The IAA of the RDFCS begins with a fault tree analysis of the system function. As shown in table 2.2-1, the fault tree analysis has several functions. The first function is to assure that no system component has any failure mode which can result in system failure. Most of the components, such as the sensors and servos, have only a few failure modes which can be observed at the interfaces with the rest of the system. For these components, the fault tree analysis provides assurance that no failure modes can cause system failure. The assurance is obtained by reviewing the completed tree and determining that system failure can only occur as a result of multiple failures.

In general, digital modules (and therefore digital components) can have a substantial number of different failure modes. In such cases, it becomes quite laborious to continue the fault tree development to a level of detail sufficient to confirm that none of those failure modes can cause system failure. The second function of fault tree analysis is to identify which digital modules are involved in performing critical functions. The task of assuring that no single module level failure can cause system failure is performed with FMEA.

A major benefit of fault tree analysis is that it focuses on the functions performed by the system elements, including those system elements involved in detecting faults and providing appropriate annunciation to the flight crew. Consequently, the third function of fault tree analysis is to confirm the adequacy of monitoring (i.e., fault detection and annunciation) in the system.

Fault tree analysis is also used to identify specific software functions required for system operation, including fault monitoring implemented in software. The software test requirements for these functions are then specifically reviewed to confirm that these requirements are adequate. This fourth function of fault trees is illustrated and discussed in greater detail as the tree for the RDFCS is developed.

The fifth function of fault tree analysis is to provide an alternate means of computing the probability of system failure. This provides a check of the probability obtained from the reliability analysis. In the subject study, the fault tree analysis verified the probability obtained from the CARSRA program to ensure that the CARSRA input does not have errors which would produce a false low probability of system failure.

### 3.4. Failure Mode and Effect Analysis Role in Integrated Assurance

Fault tree analysis provides assurance that most system components, such as analog sensors and servos, have no single failure mode which produces system failure. This is because such components have only a few possible failure modes, and it frequently is not necessary to distinguish in the fault tree among these modes. When it is necessary to distinguish among modes, it is usually fairly simple to identify the modes which are relevant in the branch of the tree being developed. The analysis can often be extended below the component level to the failure modes of the individual piece-parts which comprise the component. Analysis to this very detailed level is sometimes necessary to ascertain that a component has no failure modes which could remain undetected until a second failure occurs elsewhere in the system.

However, fault tree analysis is cumbersome and inefficient if extended from system level to the IC pin level in the processor of a digital system. Essentially, this is a result of two basic characteristics of digital systems:

- Functions which are described very simply at a higher level (e.g., sensor monitoring) require a myriad of sequential operations at the IC level. These operations are required to obtain the proper data, route it to the proper registers within the Arithmetic Logic Unit (ALU) where arithmetic and logic operations are actually performed, and route the results to the proper storage register or output port. Many different ICs are involved in each of these operations.

- Many interfaces between ICs involve several pins, and it is the combination of pin states (electrically high or low) which is significant. That is, each combination of pin states represents a different data value or instruction, and the effect of a single pin being in the wrong (faulted) state depends on the state of the other (non-faulted) pins.

The net result of these characteristics of digital hardware is that there are many more integrated-circuit-level operations performed in executing the flight software than there are pin-level failure modes. In extending a fault tree analysis from failure of system-level functions to failure of IC pins, all of these detailed operations must be included and accounted for-an extremely inefficient process. Once the fault tree had been fully developed, another extremely laborious task would remain: reviewing the tree to make certain (1) that all of the failure modes of the ICs had been accounted for, and that no failure mode could remain undetected until a second failure occurred, with the combined effect of both faults producing a hazardous condition; and (2) that no failure mode could by itself produce a hazardous condition.

FMEA provides a means of systematically examining all of the potential failure modes of the ICs to confirm that none of them could cause a hazard directly or remain latent and subsequently cause a hazard in conjunction with a second failure.

## 3.5. Reliability Analysis Role in Integrated Assurance

CARSRA is an analytical reliability prediction program used in this IAA to obtain the probability of system failure (Bjurman, et al., 1976). The use of CARSRA, along with the quantitative assessment produced by evaluating the fault tree analysis, provides two independent computations of system failure probability. This reduces the risk of a false, low probability of failure being produced by a single method and the error remaining undetected.

Although CARSRA is identified specifically in the IAA used in this analysis, some other method (except fault tree analysis) could be used. If an alternate method is used, it should have sufficient configuration adaptability to produce the predicted probability of system failure without requiring simplifying assumptions which would produce a false, low prediction. According to Hitt and Eldredge, the particular fault-tolerant system attributes that reliability models should be capable of handling are the following:

- Computer design (e.g., failure modes, loss of subsets of functions)
- Dependencies between subsystems
- Number cf redundant components
- Redundancy management (e.g., active or standby spares, voting algorithms)
- Permanent, latent, and transient faults
- Fault recovery (i.e., coverage)
- Data transmission schemes and bus architectures
- Partitioning of processing functions

Some of the earlier reliability analysis models were adequate for analysis of certain types of systems. Examples of these are Tree Aided System Reliability Analysis (TASRA), Reliability Block Diagram Computer Program (RBDCP), Reliability (REL 70), and Reliability Computers (REL COMP) models that were primarily developed in the early 1970s. Later models such as, Automated Reliability Interactive Estimation System (ARIES) (Ng and Avizienis, 1978), Computer Aided Reliability Evaluator (CARE II) (NASA, NASI-12668, March 1974), CARSRA (Bjurman, et al., 1976), and Complimentary Analytic Simulative Technique (CAST) (Conn et al., 1977) offered expanded capabilities that were more adaptable to systems having more components and greater complexity. CARE III and an improved ARIES are examples of the continuing evolution.

The certification engineer must choose the appropriate reliability analysis model based on the ability of that model to represent the system to be analyzed. In the event that a suitable match cannot be made, manual analysis may be the only alternative.

### 3.6. Fault Insertion Role in Integrated Approach

Fault insertion is used in this IAA for three purposes as shown in table 2.2-1.

- Faults are inserted, on a sampling basis, to confirm the fault effects reflected in the fault tree analysis and fault effects determined during FMEA. This includes faults of components (sensors and servos in this study) and faults of ICs (pin-level faults in the digital processor).

- Faults are inserted, also on a sampling basis, to confirm fault detection and annunciation functions implemented in the system. Many of these are also inserted to confirm fault effects.

- Faults are inserted to determine the effect when the analysis is intractable or when there is some uncertainty in the analysis result.

# 4. FAULT TREE ANALYSIS

## 4.1. General Comments

The role of fault tree analysis in the IAA was specified in section 3.3. Appendix 1 of AC 25.1309-1 stipulates that for the purpose of conducting failure analyses, "the format of quantitative analyses, which use NUREG-0492 as a guide, will be acceptable to the FAA." NUREG-0492 is a textbook for fault tree analysis published for those unfamiliar with the concepts of systems analysis. It is titled "Fault Tree Handbook," and contains an excellent bibliography on the entire subject of reliability.

## 4.2. Fault Tree Development

AC 25.1309-1 defines fault tree analysis as "a top down deductive analysis identifying the conditions and functional failures necessary to cause a defined failure condition." The fault tree, when defined for the entire system failure state, may be used to mathematically determine a system failure probability by proper consideration of the failure probabilities of all contributing events.

Fault tree analysis is a structured method of "exploding" a top-level fault into all external events, conditions, or lower-level faults that contribute to it. The top-level fault may be a system failure or a component failure. In the former case, the lower-level faults are component faults; in the latter, piece-part faults. If they are not elementary, component faults may then be recursively exploded into their respective causative elements. The topology of the resulting graph (fault tree) permits the evaluation of the combinations of external events, conditions, or faults that cause the top-level fault.

In complex systems, the graphs become so cumbersome that user aids are necessary. One such aid is the "cut set." The "cut set" is the combination of lower-level events that result in a certain higher-level failure. The procedure for obtaining cut sets may either be manual or automated. The length of a cut set portrays the levels of redundancy in the system design. Minimal cut sets are important in that they show the minimum levels of redundancy. Minimal cut sets simplify the computation of the probability of failure of the respective top-level event.

The fault tree analysis contained in this section is based on the RDFCS being in the failure condition stipulated in section 2.2: simply, during a crucial flight landing phase, when the human pilot may not complete the landing, the RDFCS fails. In the following analysis this time period will be referred to as the "crucial phase."

The analysis begins with the RDFCS in the dual-dual configuration. The system is placed in this configuration by depressing the ILS push-button. The use of the ILS push-button results in the selection of the Approach/Land (A/L) mode.

After this switch has been momentarily depressed, the A/L mode is transmitted to the FCCs and latched in. The switch is no longer needed, and therefore does not enter into the analysis.

Figures 4.2-1 through 4.2-12 contain a partial fault tree analysis of the RDFCS during the crucial phase. The numbers in engineering notation appearing at nodal points are failure probabilities and will be used in sections 4.3 and 7.2.

The top event of figure 4.2-1, Unacceptable Deviation from Path/Altitude/ Speed Profile during Crucial Flight Phase, may be considered as equivalent to RDFCS failure. This event can be caused by any of three conditions or subevents. For convenience, these can be referred to as Level-2 events with the top event considered to be at Level-1. The Level-2 events are shown as the middle row in figure 4.2-1. The first of these is that the system design is in some manner deficient for the environmental conditions encountered. This includes the possibility that the conditions encountered are outside of the system design requirements. It also includes the possibility that the control laws are deficient for some conditions which may be expected. This possibility is outside the scope of this tutorial and is not pursued here. Mulcare et al., (1979) and DOT/FAA/CT-82/140 (1982) address this subject. In particular, section 3.3.1.3. of Mulcare et al., (1979), discusses establishing an upper bound on the probability of a deficient control law by statistical methods.

The second of the Level-2 events occurs if the airplane enters the crucial phase with the RDFCS not fail-operational, and then a component failure occurs which prevents the system from completing the landing.

The third of the Level-2 events is that the crucial phase is entered with a fail-operational RDFCS, but multiple component failures occur before the end of the phase, and these failures result in RDFCS system failure.

The second of the Level-2 events, that the crucial phase is initialized without fail-operational capability, is expanded into three relevant functional areas or Level-3 events: sensing aircraft altitude and position, computing required outputs, and servo response to computed commands. The first of these, the sensing function, is expanded in figure 4.2-2 into the various parameters needed by the FCCs in the automatic landing control laws. At this and higher levels, the fault tree is functionally oriented: failures are in terms of loss of function rather than loss of hardware.

The fault tree stub of figure 4.2-3 extends the sensing function for normal acceleration to the individual hardware elements used to measure the acceleration and transmit it to the computers. The failure of that normal acceleration signal No. 1 to be present in all computer channels can be caused by loss of the sensor itself, associated wiring, or one of the circuit cards involved in receiving the signal and transmitting it to all channels. The A24 Autoland Sensor Input and A27 Discrete Input Cards are both involved. The A24 card handles the analog acceleration signal and the A27 card handles the validity discrete signal. The processor itself is not involved in the data acquisition process and so is not shown. At this level, the transition has been made from required functions to the hardware which perform these functions.

Failure of the system to provide a NO DUAL annunciation is shown in figure 4.2-4. This figure is of particular interest because of the explicit software function identified. A failure rate of zero is assigned to failure of this function, because it can be explicitly and exhaustively tested. Once it has been so tested, the probability of both NO DUAL annunciations failing because of a generic software error is taken to be zero. A generic software error is a discrepancy in the software that will cause all computer channels which use that software to produce the same, but wrong, result. Multiple computer channels do not provide redundancy with respect to generic software errors as long as the same software is used in all channels (as it is in most contemporary systems) including the RDFCS. DOT/FAA/CT-82/140 may be consulted for a discussion of software errors, and RTCA Document DO-178 should be consulted for a discussion of software test requirements.

Fault tree stubs similar to that shown in figure 4.2-3 were developed for the other sensors of figure 4.2-2. These are very much like the stub shown in figure 4.2-3 and so are not included in this tutorial.

The second of the Level-3 events of figure 4.2-1 is initiation of the crucial flight phase without fail-operational computing capability, and that an additional component failure causes system failure before the phase is complete. This is shown in figure 4.2-5 as four Level-4 events. The first of these, that channel A of FCC No. 1 fails above alert height, can be caused by either channel of the FCC failing to produce a required output, as shown by the eight events at the lowest level (Level-5) in figure 4.2-5.

Figure 4.2-6 continues the development of the fault tree for one of the Level-5 events of figure 4.2-5. This event, failure of the A channel of FCC No. 1 to produce a rudder command, can be caused by failure of any one of several cards within the channel. In this study, the two cards which make up the processor were considered in more depth than the others. These two, the A13 Control Card and the A14 Data Path Card, are shown in figures 4.2-7 and 4.2-8, respectively. Also shown in each of figures 4.2-7 and 4.2-8 is a subevent for failure of a miscellaneous part, such as the circuit board, the edge connector, or other part which is not included in one of the modules named in the other blocks.

Theoretically, the fault tree analysis of the failure of the processor to compute the rudder command can be continued below the module level to the individual IC pins or discrete piece-parts. The desirability of doing this is questionable, however, because of the nature of the processor. The processor is not designed to perform a single specific function, such as computing rudder commands. It is designed to efficiently perform a number of simple functions, such as addition, multiplication, and logic operations. A suitable sequence of such operations (i.e., the flight software) is used to make the processor generate the rudder command, the aileron command, and so forth. It is much easier to relate the modules and ICs to the simple functions (addition, multiplication) than to relate them to the more complicated functions of computing the command for a particular servo.

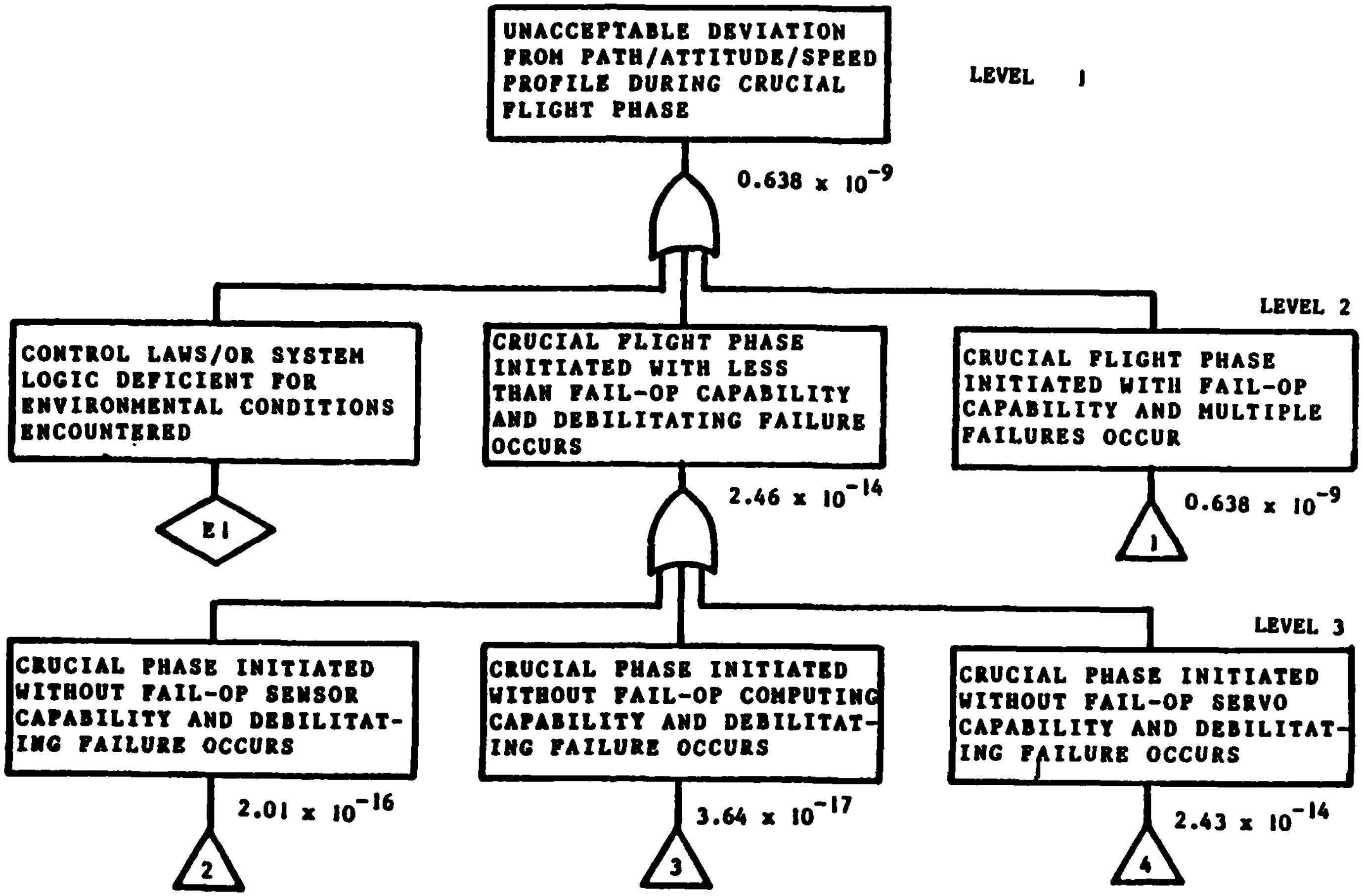

UNACCEPTABLE DEVIATION FROM PATH/ATTITUDE/SPEED PROFILE DURING CRUCIAL FLIGHT PHASE
LEVEL 1
0.638 x $10^{-9}$
LEVEL 2
CONTROL LAWS/OR SYSTEM LOGIC DEFICIENT FOR ENVIRONMENTAL CONDITIONS ENCOUNTERED
E1
CRUCIAL FLIGHT PHASE INITIATED WITH LESS THAN FAIL-OP CAPABILITY AND DEBILITATING FAILURE OCCURS
2.46 x $10^{-14}$
CRUCIAL FLIGHT PHASE INITIATED WITH FAIL-OP CAPABILITY AND MULTIPLE FAILURES OCCUR
0.638 x $10^{-9}$
1
LEVEL 3
CRUCIAL PHASE INITIATED WITHOUT FAIL-OP SENSOR CAPABILITY AND DEBILITATING FAILURE OCCURS
2.01 x $10^{-16}$
2
CRUCIAL PHASE INITIATED WITHOUT FAIL-OP COMPUTING CAPABILITY AND DEBILITATING FAILURE OCCURS
3.64 x $10^{-17}$
3
CRUCIAL PHASE INITIATED WITHOUT FAIL-OP SERVO CAPABILITY AND DEBILITATING FAILURE OCCURS
2.43 x $10^{-14}$
4

FIGURE 4.2-1. FAULT TREE TOP LEVEL

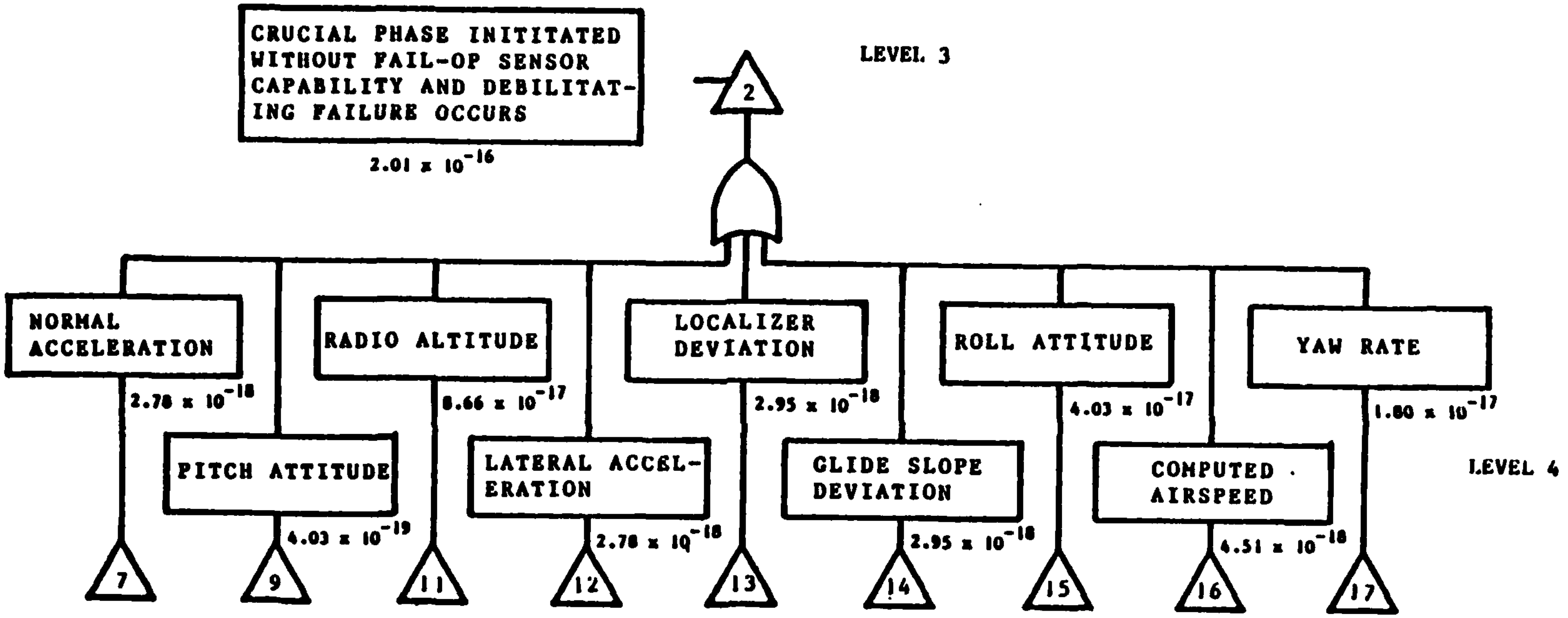


FIGURE 4.2-2. SENSING FUNCTION

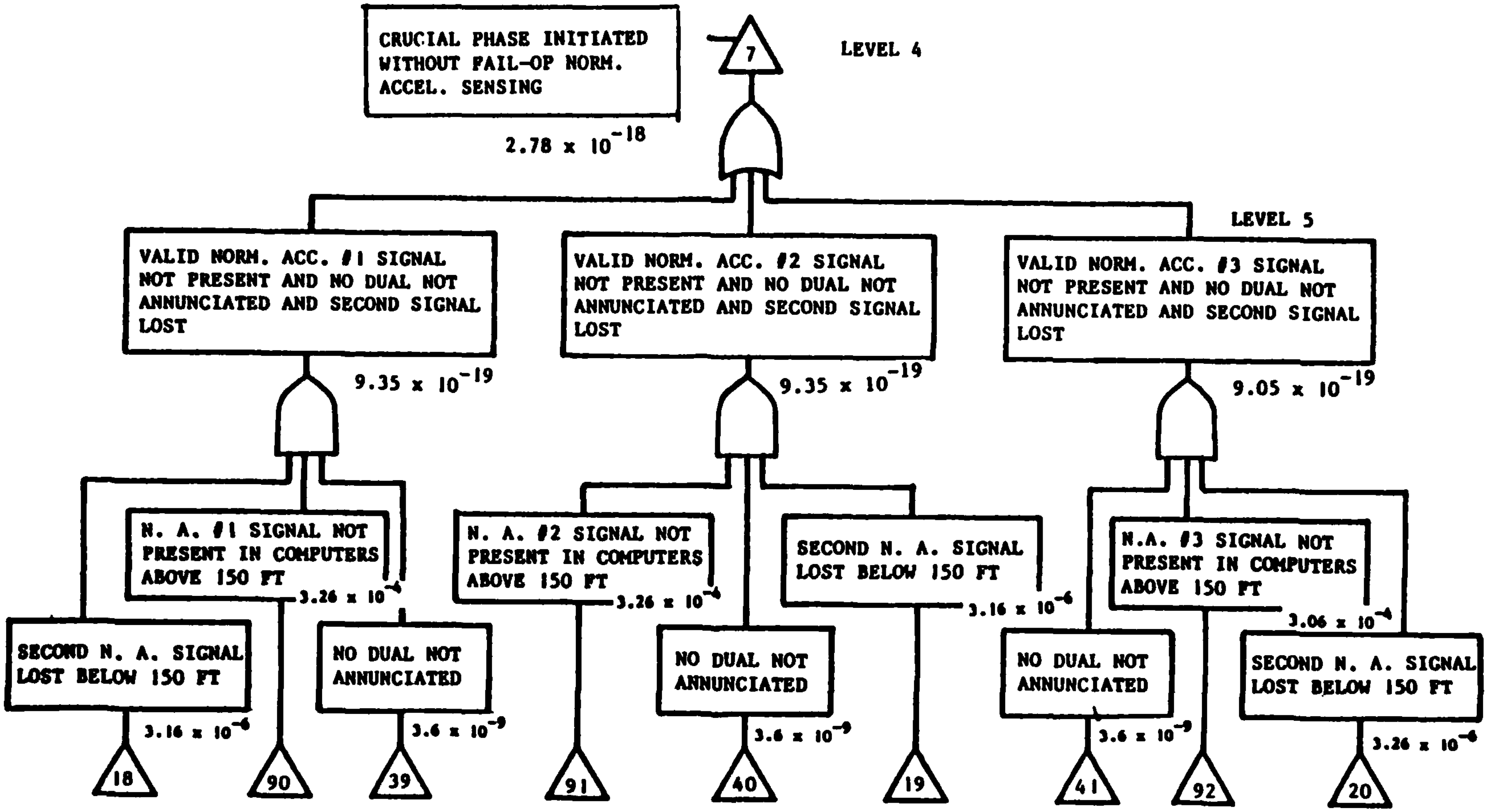

CRUCIAL PHASE INITIATED WITHOUT FAIL-OP NORM. ACCEL. SENSING
2.78 x 10^-18
7
LEVEL 4
LEVEL 5
VALID NORM. ACC. #1 SIGNAL NOT PRESENT AND NO DUAL NOT ANNUNCIATED AND SECOND SIGNAL LOST
9.35 x 10^-19
VALID NORM. ACC. #2 SIGNAL NOT PRESENT AND NO DUAL NOT ANNUNCIATED AND SECOND SIGNAL LOST
9.35 x 10^-19
VALID NORM. ACC. #3 SIGNAL NOT PRESENT AND NO DUAL NOT ANNUNCIATED AND SECOND SIGNAL LOST
9.05 x 10^-19
N. A. #1 SIGNAL NOT PRESENT IN COMPUTERS ABOVE 150 FT
3.26 x 10^-4
SECOND N. A. SIGNAL LOST BELOW 150 FT
3.16 x 10^-6
NO DUAL NOT ANNUNCIATED
3.6 x 10^-9
N. A. #2 SIGNAL NOT PRESENT IN COMPUTERS ABOVE 150 FT
3.26 x 10^-4
NO DUAL NOT ANNUNCIATED
3.6 x 10^-9
SECOND N. A. SIGNAL LOST BELOW 150 FT
3.16 x 10^-6
N.A. #3 SIGNAL NOT PRESENT IN COMPUTERS ABOVE 150 FT
3.06 x 10^-4
NO DUAL NOT ANNUNCIATED
3.6 x 10^-9
SECOND N. A. SIGNAL LOST BELOW 150 FT
3.26 x 10^-6
18
90
39
91
40
19
41
92
20

FIGURE 4.2-3. NORMAL ACCELERATION SENSING (1 of 3)

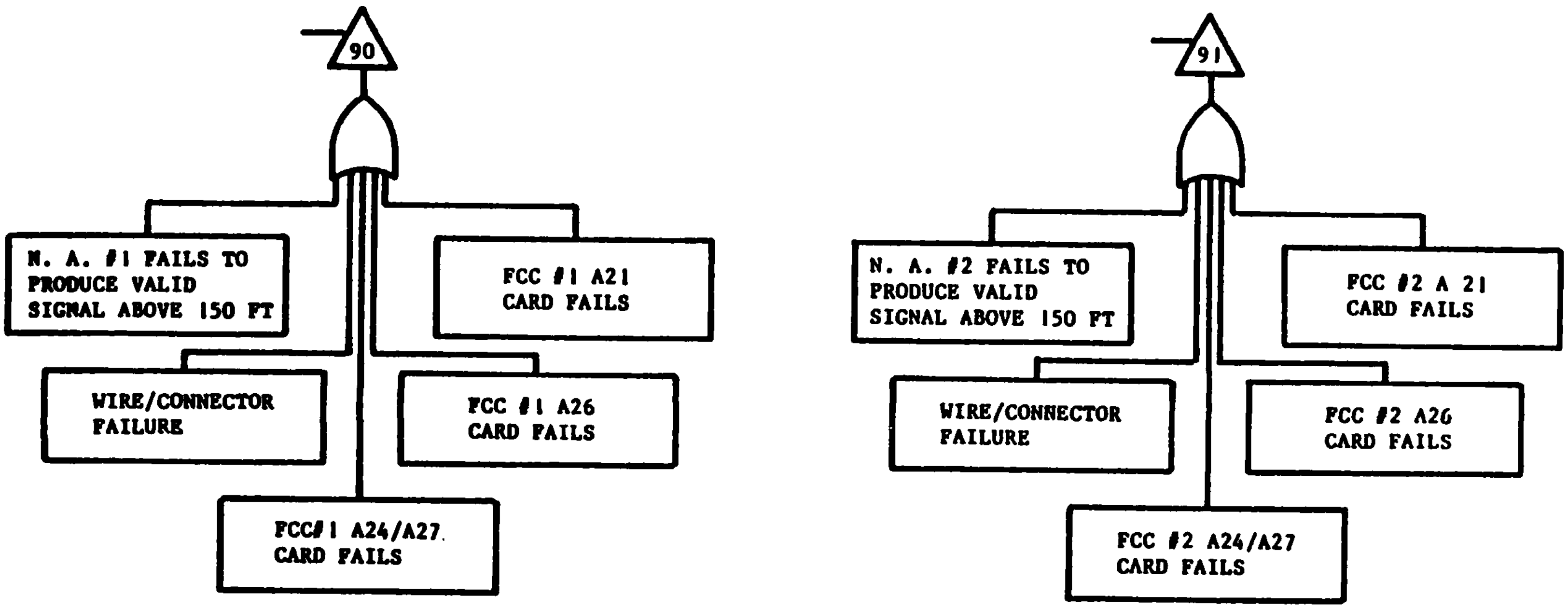


FIGURE 4.2-3. NORMAL ACCELERATION SENSING (2 of 3)

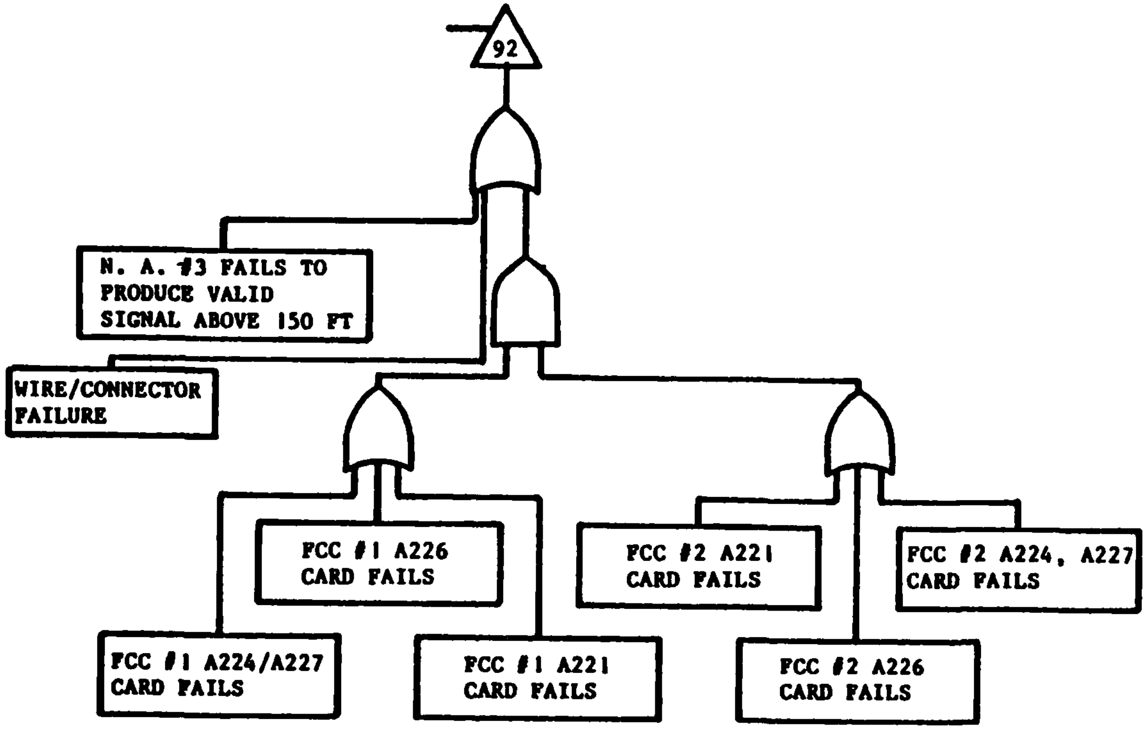


FIGURE 4.2-3. NORMAL ACCELERATION SENSING (3 of 3)

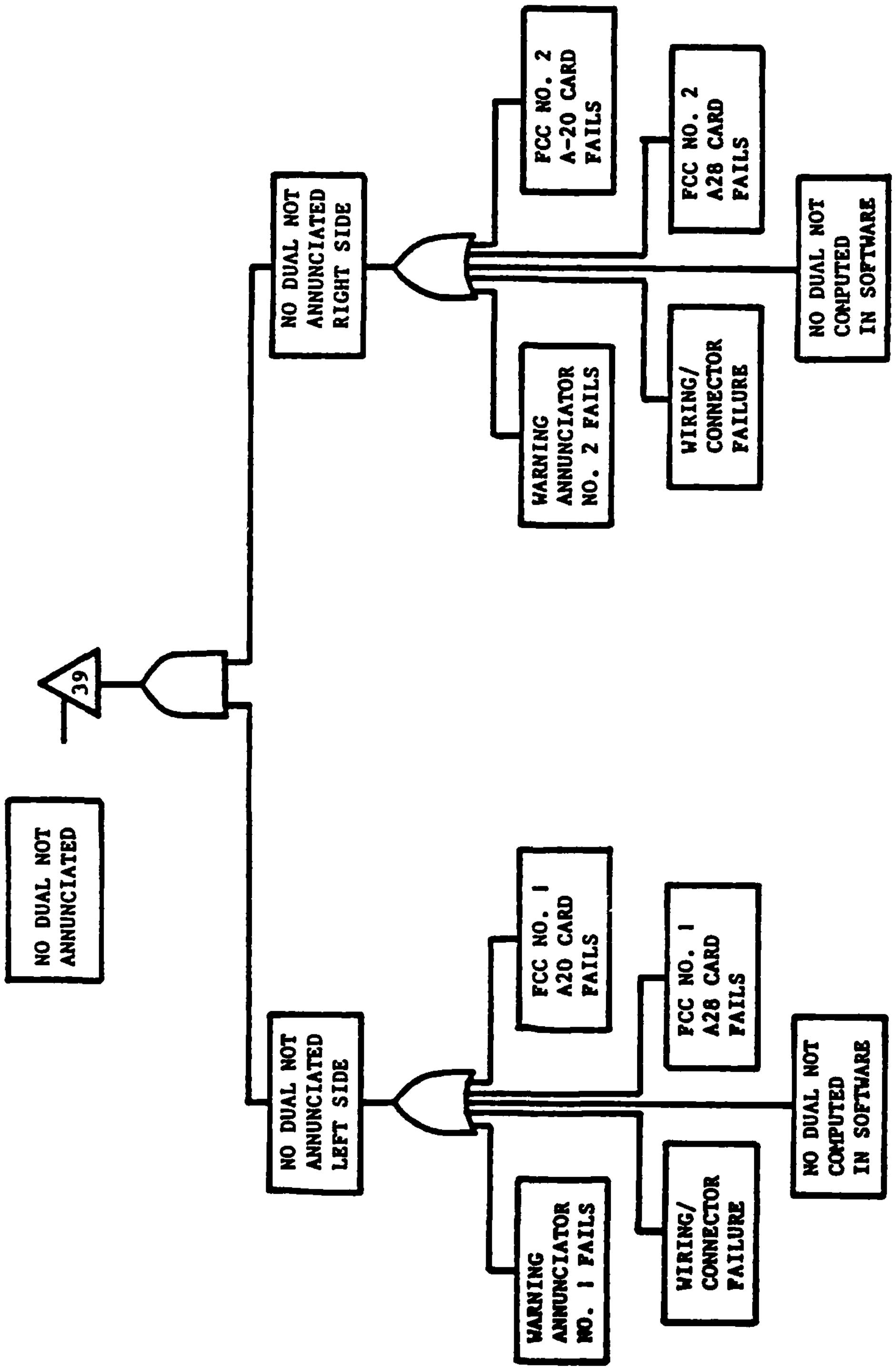

NO DUAL NOT ANNUNCIATED
39
NO DUAL NOT ANNUNCIATED LEFT SIDE
FCC NO. 1 A20 CARD FAILS
FCC NO. 1 A28 CARD FAILS
NO DUAL NOT COMPUTED IN SOFTWARE
WIRING/ CONNECTOR FAILURE
WARNING ANNUNCIATOR NO. 1 FAILS
NO DUAL NOT ANNUNCIATED RIGHT SIDE
FCC NO. 2 A-20 CARD FAILS
FCC NO. 2 A28 CARD FAILS
NO DUAL NOT COMPUTED IN SOFTWARE
WIRING/ CONNECTOR FAILURE
WARNING ANNUNCIATOR NO. 2 FAILS

FIGURE 4.2-4. NO DUAL ANNUNCIATION

It is also easier, in general, to relate a specific failure mode of an IC within the processor to its effect on the processor operation than to start with the effect and then work in the other direction to the IC failure modes which would produce the effect. In other words, it is easier to do an FMEA than a fault tree analysis at this level. FMEA will be discussed in section 5.

Another reason for preferring FMEA to fault trees at this level is that in the course of performing the fault tree analysis, the analyst must account for all of the ways the processor can fail; that is, all of the ways in which the processor output can be wrong.

These ways are the failure modes of the processor. Each of these modes must then be traced to all possible combinations of IC pin failures which could produce the processor failure mode. Because processors have many different possible outputs, there are a high number of ways that the output could be wrong. There is no practical way of assuring that all of these possibilities have actually been covered in the fault tree. The FMEA requires that all pin-level IC failure modes be considered. These modes are much better understood, and there are fewer of them, so that it is much easier to be certain that they have all been covered. This is not meant to imply that a complete pin-level FMEA is easy or inexpensive; it is neither.

Due to the above considerations, the fault tree analysis of the processor was not continued below the level developed in figures 4.2-7 and 4.2-8. Instead, the FMEA approach was used as described in section 5.

To continue with the development of other branches of the fault tree, figure 4.2-9 develops the event of figure 4.2-6 in which the pilot is not warned that FCC No. 1 A channel is not generating a correct rudder command. This portion of the fault tree includes several software functions. In a production program, the test requirements of each of these functions should be reviewed to confirm that they satisfy the criteria of RTCA Document DO-178. In this tutorial, conducted for illustrative purposes, this review was not made.

Tree stubs similar to that developed in figures 4.2-6 through 4.2-9 were developed for the other required outputs from Channel A of FCC No. 1 and the other three channels (figure 4.2-5). They are not included here because they repeat the analysis shown.

The last of the Level-3 events of figure 4.2-1 is that the crucial phase is initiated without fail-operational servo capability, and a debilitating failure occurs. This is expanded in figure 4.2-10 into the three aircraft control axes: roll, pitch, and yaw. Figure 4.2-11 shows the fault tree for failure of the No. 1 yaw autopilot servo, with the servo failure not annunciated to the crew.

Fault tree stubs for the other five servos of figure 4.2-10 were developed to complete the analysis of the Level-3 events of figure 4.2-1. These are similar to the stub shown for the rudder servo and are not included in this discussion. This completes the discussion of the second of the Level-2 events of figure 4.2-1.

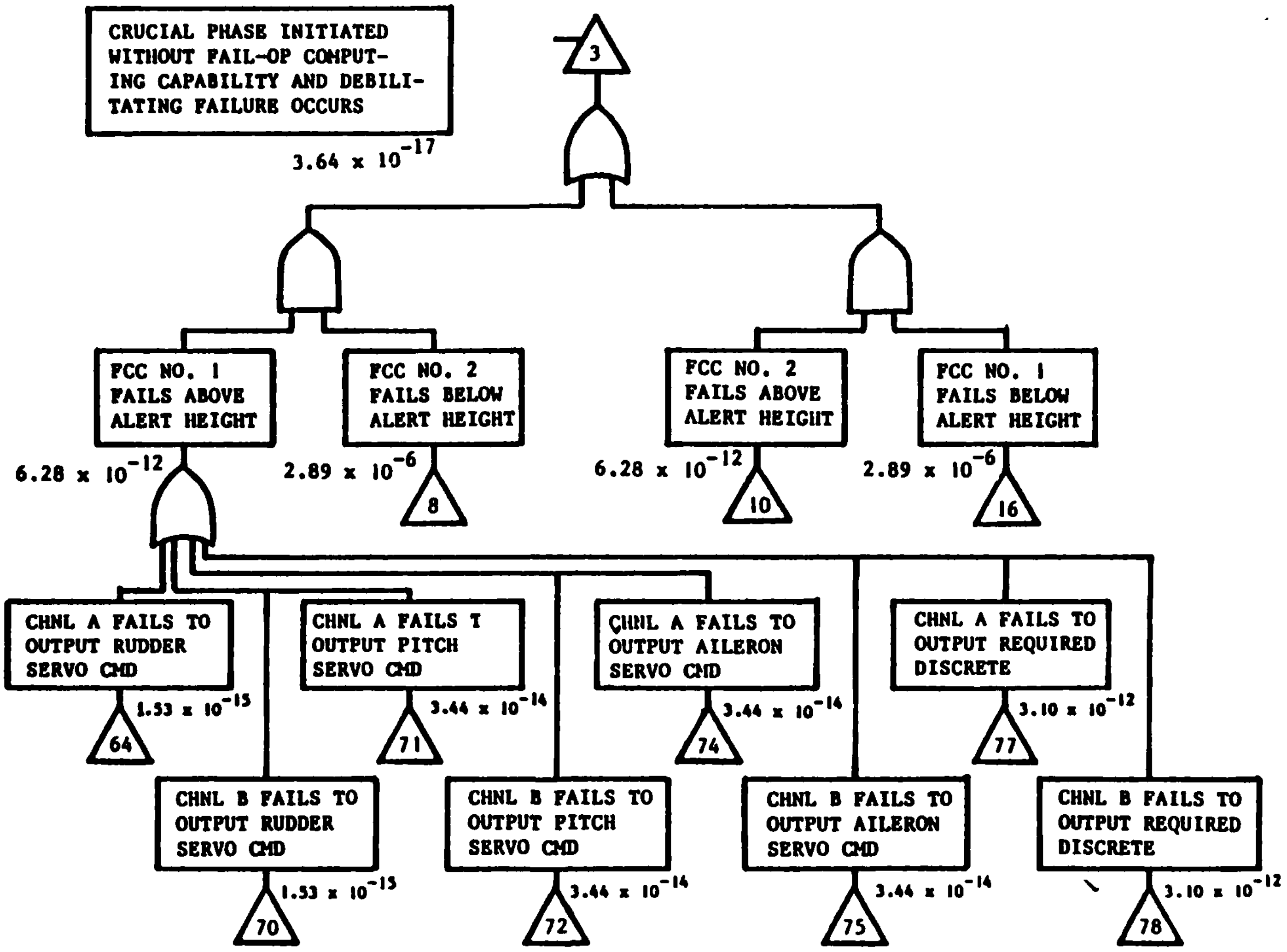

CRUCIAL PHASE INITIATED WITHOUT FAIL-OP COMPUTING CAPABILITY AND DEBILITATING FAILURE OCCURS
3.64 x 10$^{-17}$
3
FCC NO. 1 FAILS ABOVE ALERT HEIGHT
6.28 x 10$^{-12}$
FCC NO. 2 FAILS BELOW ALERT HEIGHT
2.89 x 10$^{-6}$
8
FCC NO. 2 FAILS ABOVE ALERT HEIGHT
6.28 x 10$^{-12}$
10
FCC NO. 1 FAILS BELOW ALERT HEIGHT
2.89 x 10$^{-6}$
16
CHNL A FAILS TO OUTPUT RUDDER SERVO CMD
1.53 x 10$^{-15}$
64
CHNL A FAILS T OUTPUT PITCH SERVO CMD
3.44 x 10$^{-14}$
71
CHNL A FAILS TO OUTPUT AILERON SERVO CMD
3.44 x 10$^{-14}$
74
CHNL A FAILS TO OUTPUT REQUIRED DISCRETE
3.10 x 10$^{-12}$
77
CHNL B FAILS TO OUTPUT RUDDER SERVO CMD
1.53 x 10$^{-15}$
70
CHNL B FAILS TO OUTPUT PITCH SERVO CMD
3.44 x 10$^{-14}$
72
CHNL B FAILS TO OUTPUT AILERON SERVO CMD
3.44 x 10$^{-14}$
75
CHNL B FAILS TO OUTPUT REQUIRED DISCRETE
3.10 x 10$^{-12}$
78

FIGURE 4.2-5. COMPUTING FUNCTION

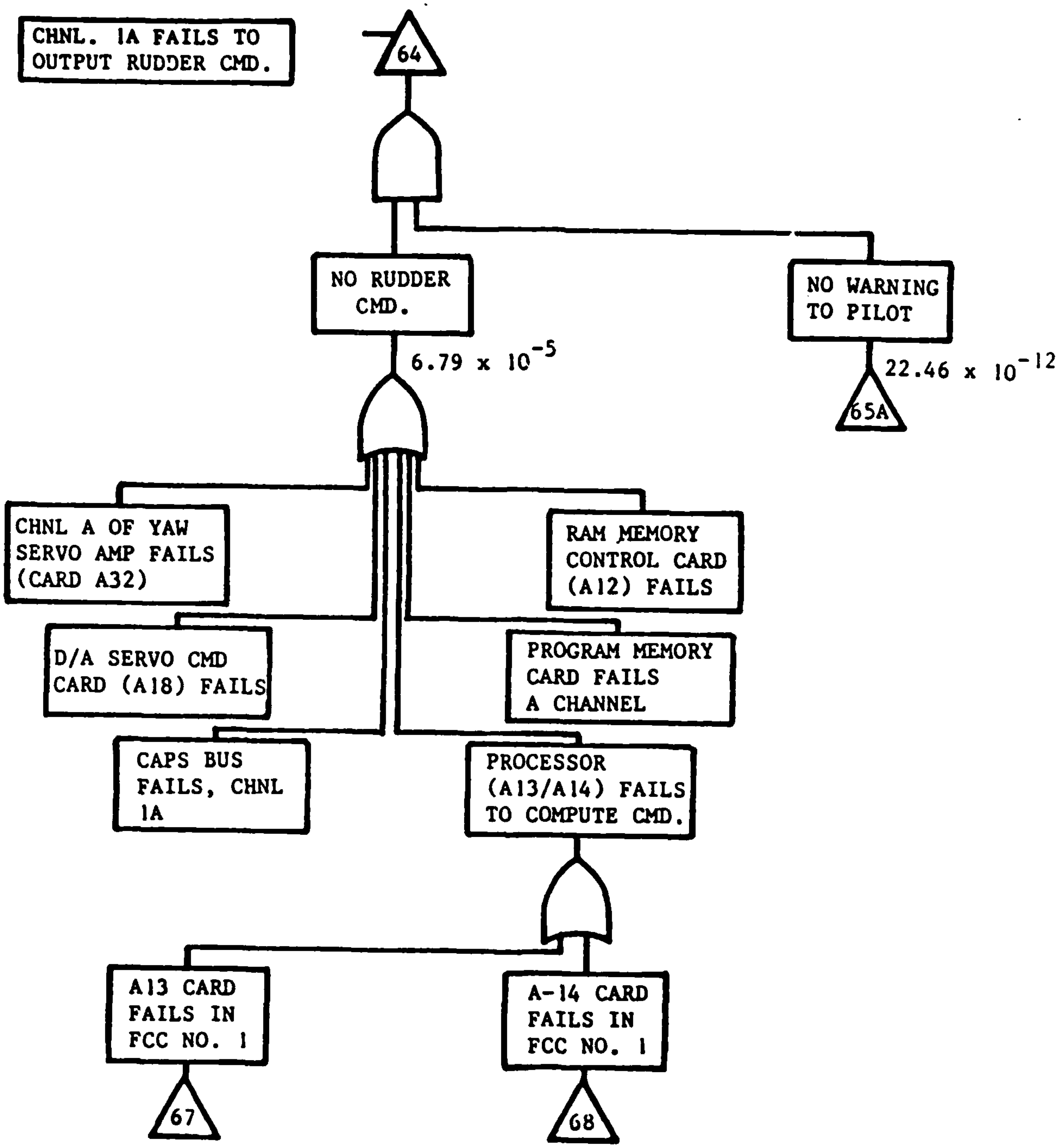

CHNL. 1A FAILS TO OUTPUT RUDDER CMD.
64
NO RUDDER CMD.
6.79 x 10$^{-5}$
NO WARNING TO PILOT
22.46 x 10$^{-12}$
65A
CHNL A OF YAW SERVO AMP FAILS (CARD A32)
RAM MEMORY CONTROL CARD (A12) FAILS
D/A SERVO CMD CARD (A18) FAILS
PROGRAM MEMORY CARD FAILS A CHANNEL
CAPS BUS FAILS, CHNL 1A
PROCESSOR (A13/A14) FAILS TO COMPUTE CMD.
A13 CARD FAILS IN FCC NO. 1
A-14 CARD FAILS IN FCC NO. 1
67
68

FIGURE 4.2-6. CHANNEL 1A RUDDER COMMAND

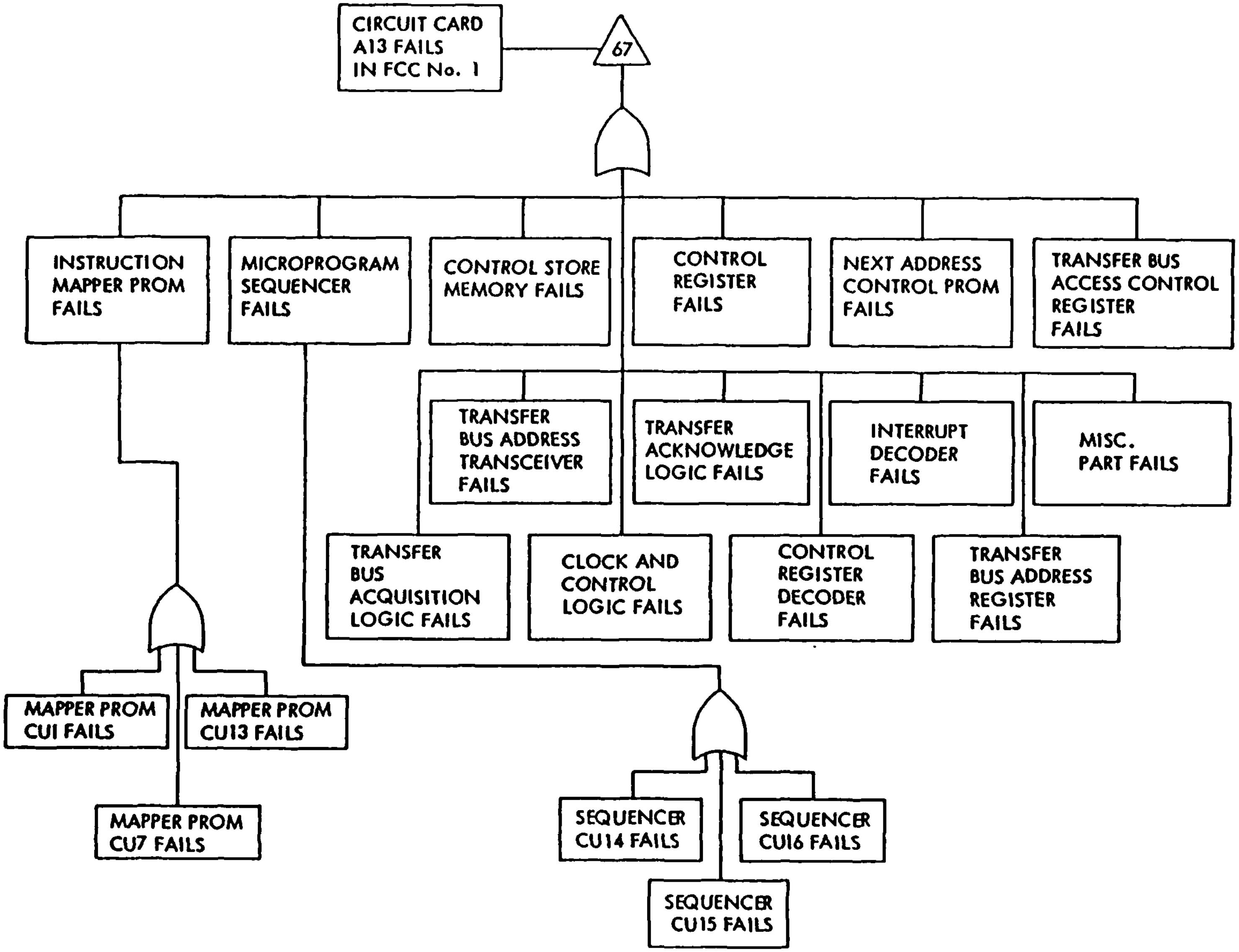

CIRCUIT CARD A13 FAILS IN FCC No. 1
67
INSTRUCTION MAPPER PROM FAILS
MICROPROGRAM SEQUENCER FAILS
CONTROL STORE MEMORY FAILS
CONTROL REGISTER FAILS
NEXT ADDRESS CONTROL PROM FAILS
TRANSFER BUS ACCESS CONTROL REGISTER FAILS
TRANSFER BUS ADDRESS TRANSCEIVER FAILS
TRANSFER ACKNOWLEDGE LOGIC FAILS
INTERRUPT DECODER FAILS
MISC. PART FAILS
TRANSFER BUS ACQUISITION LOGIC FAILS
CLOCK AND CONTROL LOGIC FAILS
CONTROL REGISTER DECODER FAILS
TRANSFER BUS ADDRESS REGISTER FAILS
MAPPER PROM CUI FAILS
MAPPER PROM CU13 FAILS
MAPPER PROM CU7 FAILS
SEQUENCER CU14 FAILS
SEQUENCER CU16 FAILS
SEQUENCER CU15 FAILS

FIGURE 4.2-7. FCC PROCESSOR CONTROL CARD

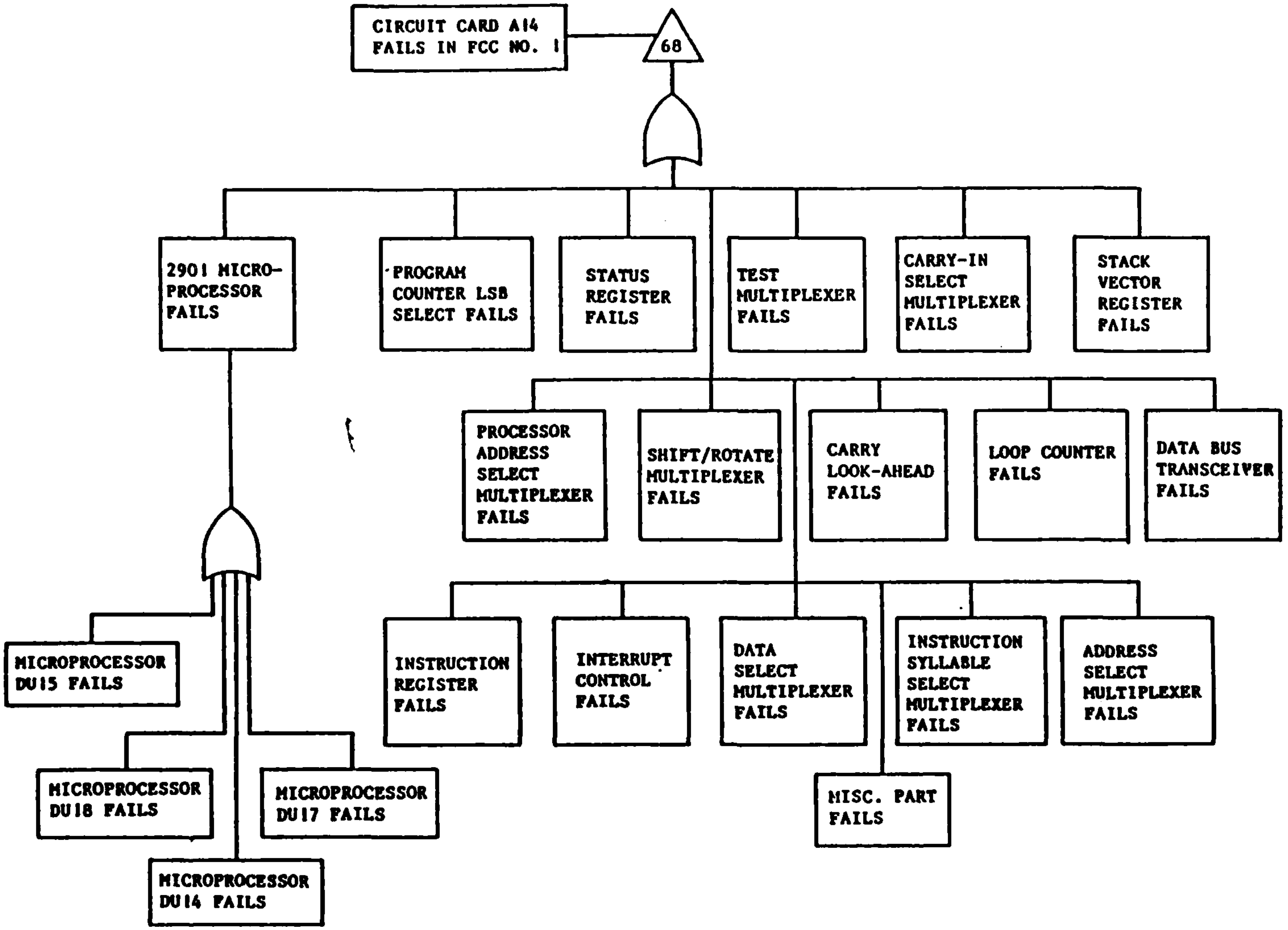

CIRCUIT CARD A14 FAILS IN FCC NO. 1
68
2901 MICRO-PROCESSOR FAILS
PROGRAM COUNTER LSB SELECT FAILS
STATUS REGISTER FAILS
TEST MULTIPLEXER FAILS
CARRY-IN SELECT MULTIPLEXER FAILS
STACK VECTOR REGISTER FAILS
PROCESSOR ADDRESS SELECT MULTIPLEXER FAILS
SHIFT/ROTATE MULTIPLEXER FAILS
CARRY LOOK-AHEAD FAILS
LOOP COUNTER FAILS
DATA BUS TRANSCEIVER FAILS
MICROPROCESSOR DU15 FAILS
MICROPROCESSOR DU18 FAILS
MICROPROCESSOR DU17 FAILS
MICROPROCESSOR DU14 FAILS
INSTRUCTION REGISTER FAILS
INTERRUPT CONTROL FAILS
DATA SELECT MULTIPLEXER FAILS
INSTRUCTION SYLLABLE SELECT MULTIPLEXER FAILS
ADDRESS SELECT MULTIPLEXER FAILS
MISC. PART FAILS

FIGURE 4.2-8. FCC PROCESSOR DATA PATH CARD

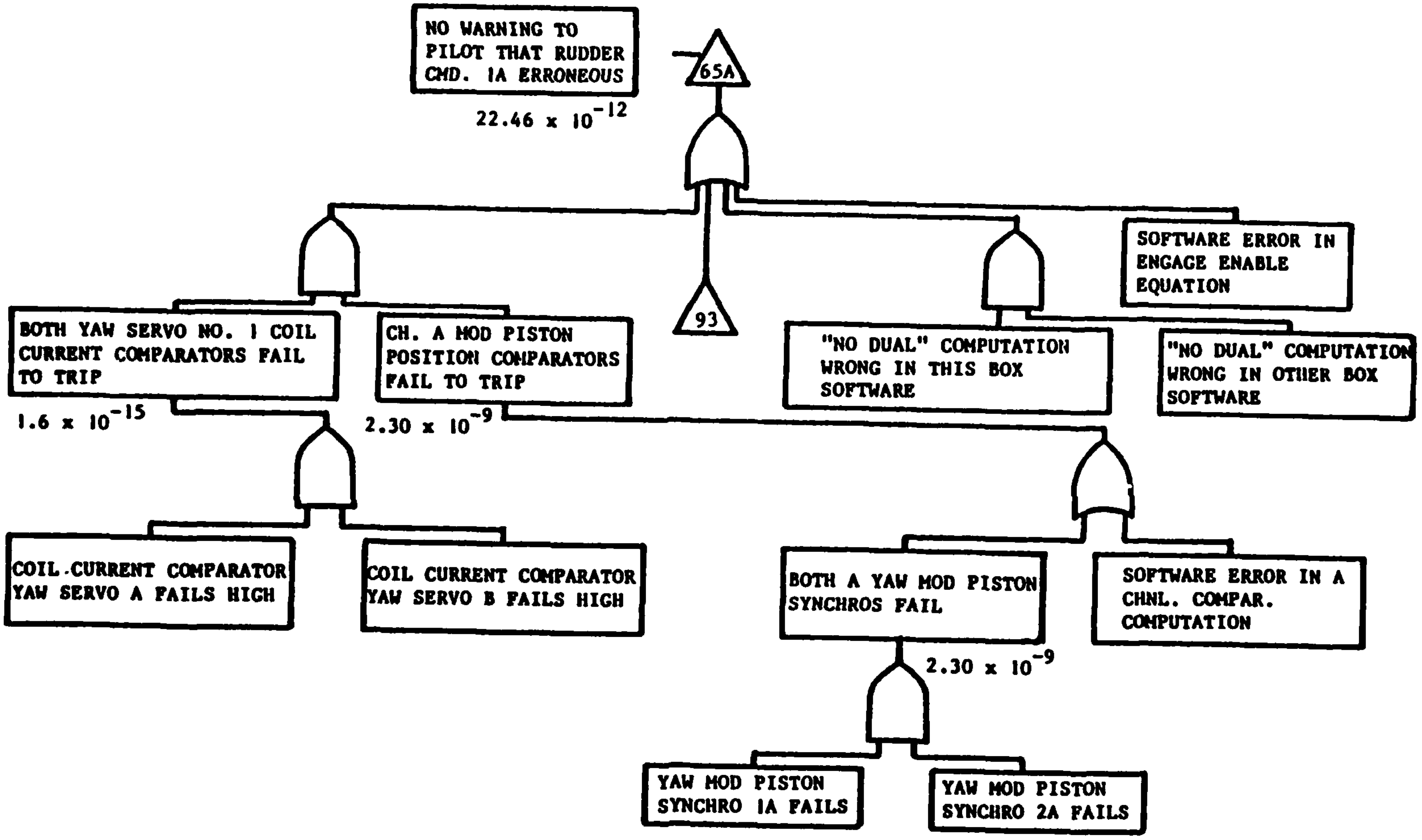

NO WARNING TO PILOT THAT RUDDER CMD. 1A ERRONEOUS
22.46 x $10^{-12}$
65A
93
BOTH YAW SERVO NO. 1 COIL CURRENT COMPARATORS FAIL TO TRIP
1.6 x $10^{-15}$
CH. A MOD PISTON POSITION COMPARATORS FAIL TO TRIP
2.30 x $10^{-9}$
"NO DUAL" COMPUTATION WRONG IN THIS BOX SOFTWARE
"NO DUAL" COMPUTATION WRONG IN OTHER BOX SOFTWARE
SOFTWARE ERROR IN ENGAGE ENABLE EQUATION
COIL.CURRENT COMPARATOR YAW SERVO A FAILS HIGH
COIL CURRENT COMPARATOR YAW SERVO B FAILS HIGH
BOTH A YAW MOD PISTON SYNCHROS FAIL
2.30 x $10^{-9}$
SOFTWARE ERROR IN A CHNL. COMPAR. COMPUTATION
YAW MOD PISTON SYNCHRO 1A FAILS
YAW MOD PISTON SYNCHRO 2A FAILS

FIGURE 4.2-9. YAW AUTOPILOT SERVO COMMAND WARNING (1 of 2)

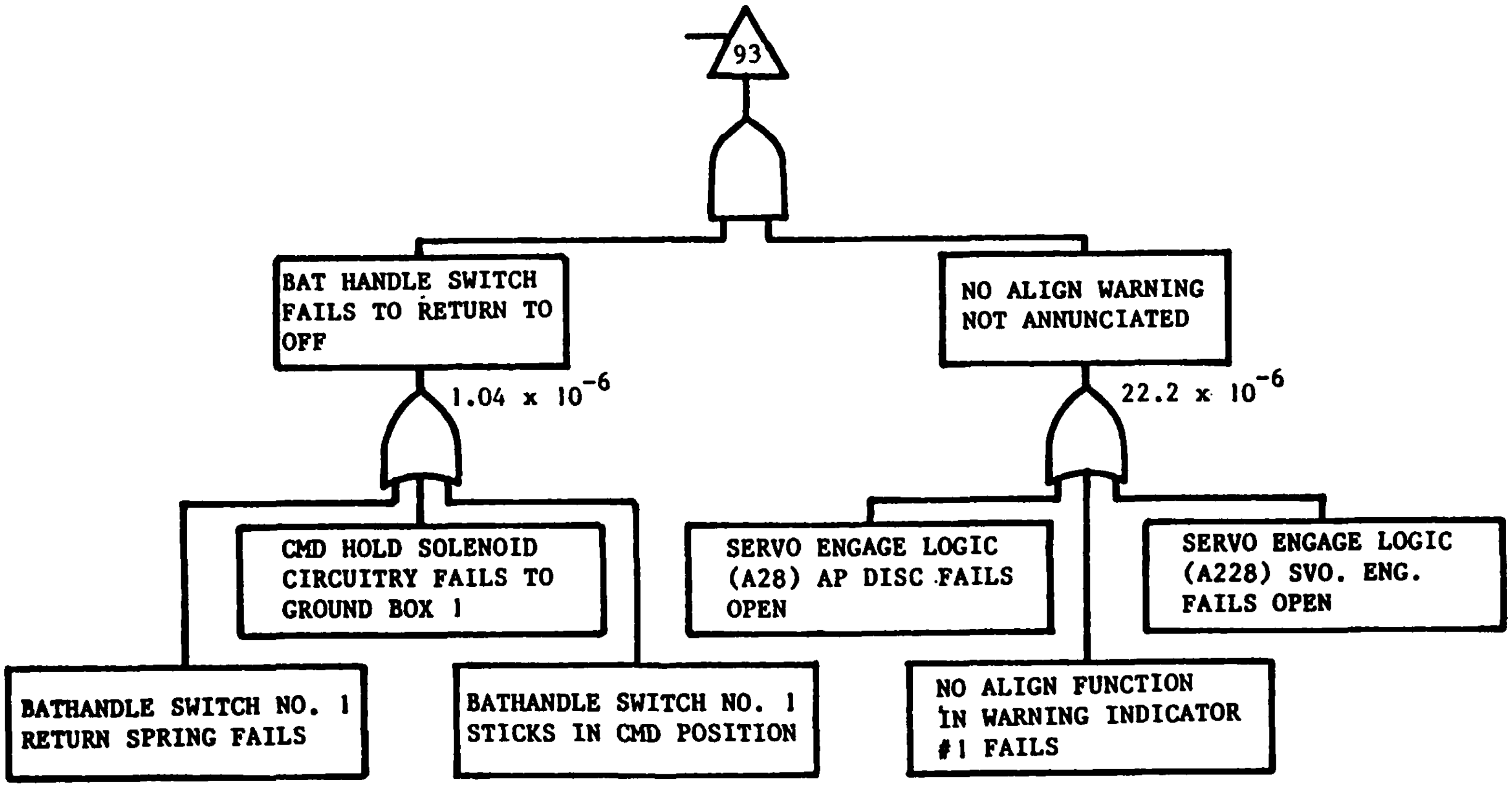

93
BAT HANDLE SWITCH FAILS TO RETURN TO OFF
1.04 x 10$^{-6}$
NO ALIGN WARNING NOT ANNUNCIATED
22.2 x 10$^{-6}$
CMD HOLD SOLENOID CIRCUITRY FAILS TO GROUND BOX 1
BATHANDLE SWITCH NO. 1 RETURN SPRING FAILS
BATHANDLE SWITCH NO. 1 STICKS IN CMD POSITION
SERVO ENGAGE LOGIC (A28) AP DISC FAILS OPEN
SERVO ENGAGE LOGIC (A228) SVO. ENG. FAILS OPEN
NO ALIGN FUNCTION IN WARNING INDICATOR #1 FAILS

FIGURE 4.2-9. YAW AUTOPILOT SERVO COMMAND WARNING (2 of 2)

The third of the Level-2 events of figure 4.2-1 is that multiple failures occur during the crucial flight phase, and these occur in a combination which causes system failure. Figure 4.2-12 shows the initial development of this event to lower levels. Continuing this development produces a major branch of the fault tree, similar to but simpler than that for the second of the Level-2 events. It differs primarily in that the NO DUAL annunciation does not appear, because that particular warning is suppressed during the crucial phase. Since that major branch is similar to that already discussed, it is not described further here.

## 4.3. Quantitative Fault Tree Analysis

System failure probability was computed from the fault tree using the hardware failure rates presented in section 7. A failure rate of zero was used for each software function, since there is currently no acceptable way of predicting DFCS software failure rates (RTCA Document DO-178, section 2.2.1).

Considering hardware failure modes only, the probability of initiating the crucial phase with less than fail-operational capability and a second failure debilitating the system was calculated to be $2.46 \times 10^{-14}$. This is based on a flight time of 4.0 hours prior to the crucial phase and a crucial phase duration of 0.02 hours. The probability of the system failing because of multiple failures during the crucial phase was calculated to be $0.638 \times 10^{-9}$. This is based on a crucial phase duration of 0.02 hours. Table 4.3-1 compares the system failure probabilities obtained from the fault tree analysis with those obtained using the CARSRA reliability prediction program. The latter will be discussed in section 8.

The system failure probabilities computed are actually upper bounds on the actual failure probabilities. This is because the fault trees are based on the assumption, for many items, that all failure modes of the item render the item incapable of performing any of its functions. For example, certain buffers on the A26 Data Acquisition Card are used for sensor data which is not required for automatic landing. So at least some of the failures of these buffers would not prevent the card from correctly handling required data. However, the failure rates used in the analysis are for the entire card, including these buffers, so that the failure probability calculated for the card includes card failure modes which would not affect automatic landing.

The computation of the probability of system failure is accomplished by a process of "rolling up" from the lowest event levels. In computing the probability of an event's failure based on its subevents' failure probabilities, consideration must be given to several factors. Among these factors are the following:

- logical structure of the event: A OR B OR C, A AND B AND C, A OR B AND C, etc. (where A, B, and C are subevents)
- dependence or independence of subevents

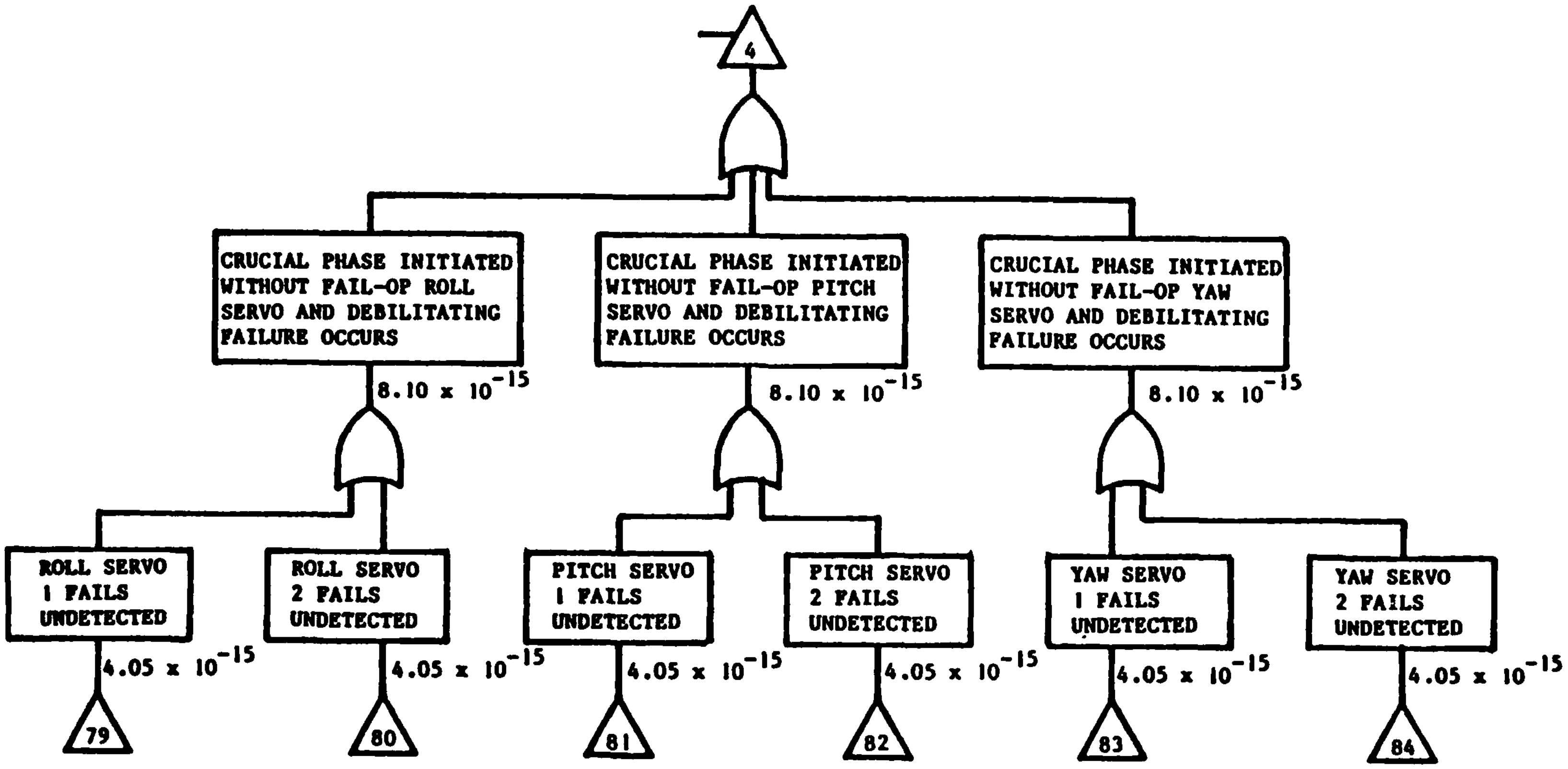
TABLE 4.3-1. QUANTITATIVE RESULTS

| Probability Of | Fault Tree Result | CARSRA Result |
|---|---|---|
| Unannunciated Failure in Cruise and Second Failure in Landing | $2.46 \times 10^{-14}$ | $3.36 \times 10^{-14}$ |
| Multiple Failures in Landing | $0.64 \times 10^{-9}$ | $0.66 \times 10^{-9}$ |

The "rolling up" process continues from the lowest-level events through the top-level event. The actual number of computations can be large. Fault-tree algorithms use minimal cut sets (see section 4.2) to reduce the computational effort.

When dealing with these complexities, the approach to probability computation should always be conservative.

Poor event and subevent definition may result in excessive common failure modes within subevents. This results in having common failure modes simultaneously affect the operation of two or more separate systems, although these systems may otherwise be independent. Some common failure modes may be unavoidable. Examples of these are losses of electrical power, hydraulic power, or cooling. *FMEA is useful in identifying common failure modes.*



4
CRUCIAL PHASE INITIATED WITHOUT FAIL-OP ROLL SERVO AND DEBILITATING FAILURE OCCURS
8.10 x 10-15
CRUCIAL PHASE INITIATED WITHOUT FAIL-OP PITCH SERVO AND DEBILITATING FAILURE OCCURS
8.10 x 10-15
CRUCIAL PHASE INITIATED WITHOUT FAIL-OP YAW SERVO AND DEBILITATING FAILURE OCCURS
8.10 x 10-15
ROLL SERVO 1 FAILS UNDETECTED
4.05 x 10-15
79
ROLL SERVO 2 FAILS UNDETECTED
4.05 x 10-15
80
PITCH SERVO 1 FAILS UNDETECTED
4.05 x 10-15
81
PITCH SERVO 2 FAILS UNDETECTED
4.05 x 10-15
82
YAW SERVO 1 FAILS UNDETECTED
4.05 x 10-15
83
YAW SERVO 2 FAILS UNDETECTED
4.05 x 10-15
84

FIGURE 4.2-10. SERVO FUNCTIONS

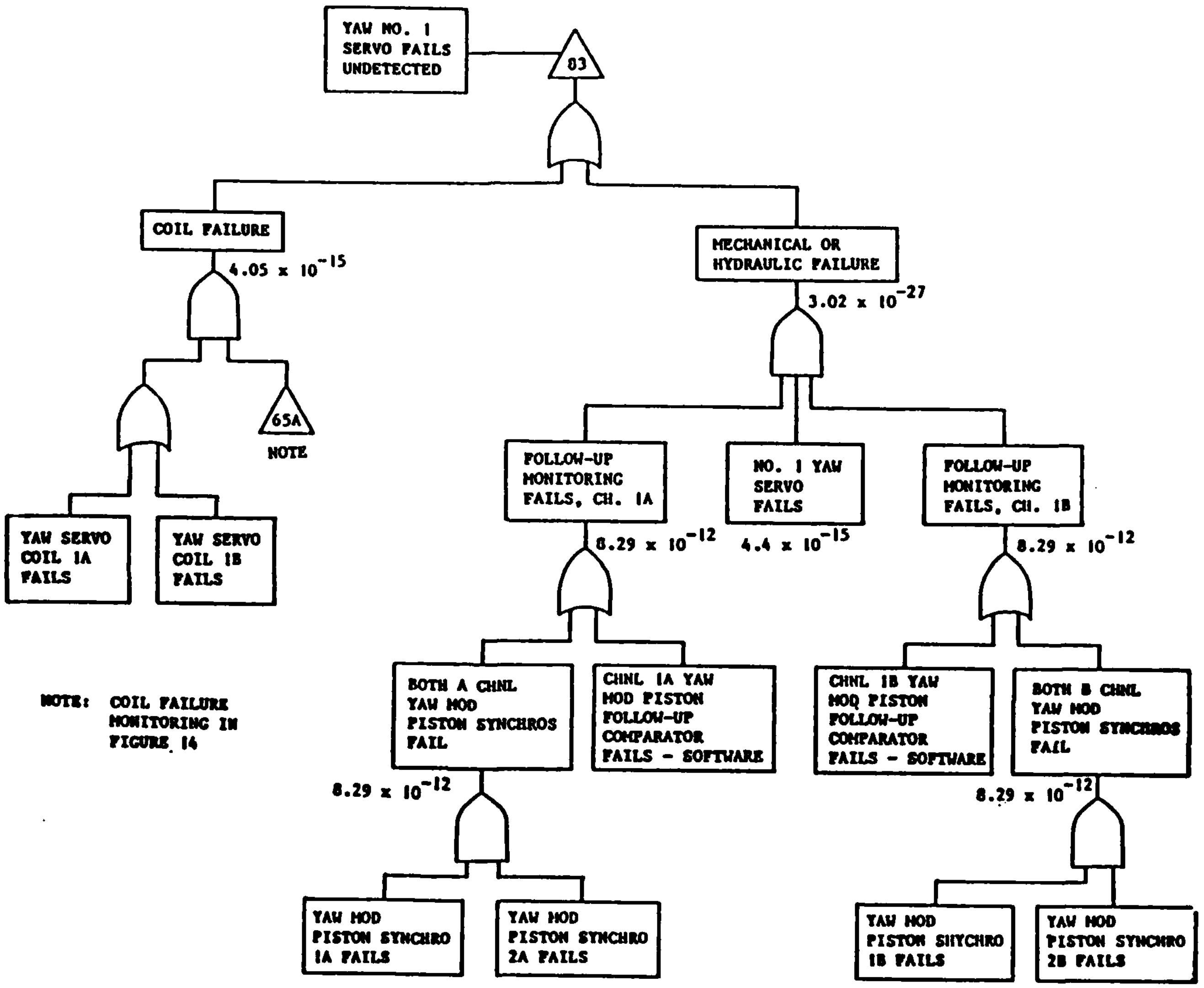

YAW NO. 1 SERVO FAILS UNDETECTED
83
COIL FAILURE
4.05 x $10^{-15}$
65A
NOTE
YAW SERVO COIL 1A FAILS
YAW SERVO COIL 1B FAILS
NOTE: COIL FAILURE MONITORING IN FIGURE 14
MECHANICAL OR HYDRAULIC FAILURE
3.02 x $10^{-27}$
FOLLOW-UP MONITORING FAILS, CH. 1A
8.29 x $10^{-12}$
NO. 1 YAW SERVO FAILS
4.4 x $10^{-15}$
FOLLOW-UP MONITORING FAILS, CH. 1B
8.29 x $10^{-12}$
BOTH A CHNL YAW MOD PISTON SYNCHROS FAIL
8.29 x $10^{-12}$
CHNL 1A YAW MOD PISTON FOLLOW-UP COMPARATOR FAILS - SOFTWARE
CHNL 1B YAW MOQ PISTON FOLLOW-UP COMPARATOR FAILS - SOFTWARE
BOTH B CHNL YAW MOD PISTON SYNCHROS FAIL
8.29 x $10^{-12}$
YAW MOD PISTON SYNCHRO 1A FAILS
YAW MOD PISTON SYNCHRO 2A FAILS
YAW MOD PISTON SHYCHRO 1B FAILS
YAW MOD PISTON SYNCHRO 2B FAILS

FIGURE 4.2-11. NO. 1 YAW AUTOPILOT SERVO

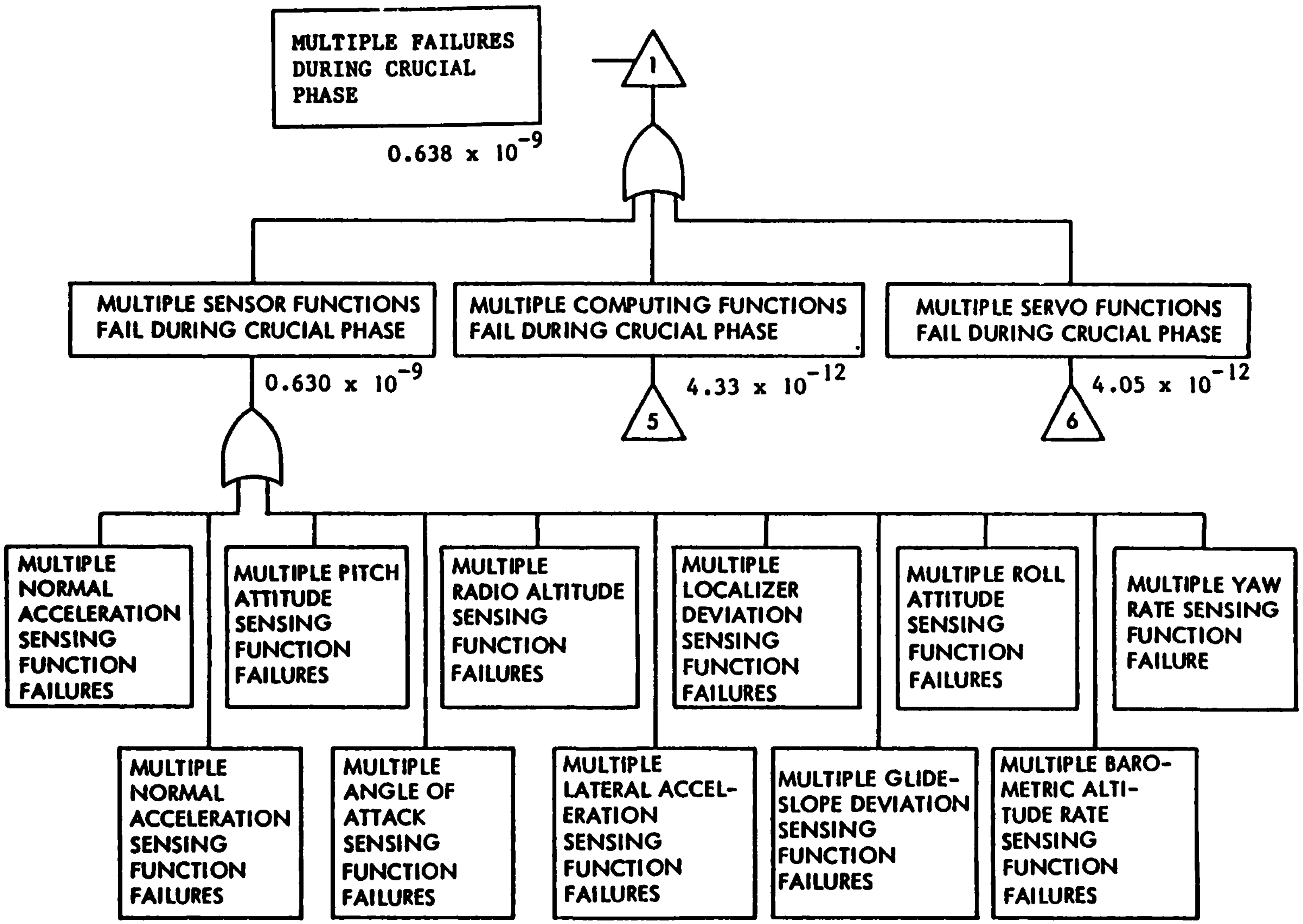

MULTIPLE FAILURES DURING CRUCIAL PHASE
1
0.638 x 10⁻⁹
MULTIPLE SENSOR FUNCTIONS FAIL DURING CRUCIAL PHASE
0.630 x 10⁻⁹
MULTIPLE COMPUTING FUNCTIONS FAIL DURING CRUCIAL PHASE
4.33 x 10⁻¹²
5
MULTIPLE SERVO FUNCTIONS FAIL DURING CRUCIAL PHASE
4.05 x 10⁻¹²
6
MULTIPLE NORMAL ACCELERATION SENSING FUNCTION FAILURES
MULTIPLE NORMAL ACCELERATION SENSING FUNCTION FAILURES
MULTIPLE PITCH ATTITUDE SENSING FUNCTION FAILURES
MULTIPLE ANGLE OF ATTACK SENSING FUNCTION FAILURES
MULTIPLE RADIO ALTITUDE SENSING FUNCTION FAILURES
MULTIPLE LATERAL ACCEL-ERATION SENSING FUNCTION FAILURES
MULTIPLE LOCALIZER DEVIATION SENSING FUNCTION FAILURES
MULTIPLE GLIDE-SLOPE DEVIATION SENSING FUNCTION FAILURES
MULTIPLE ROLL ATTITUDE SENSING FUNCTION FAILURES
MULTIPLE BARO-METRIC ALTI-TUDE RATE SENSING FUNCTION FAILURES
MULTIPLE YAW RATE SENSING FUNCTION FAILURE

FIGURE 4.2-12. MULTIPLE FAILURES DURING CRUCIAL PHASE

# 5. FAILURE MODE AND EFFECT ANALYSIS

## 5.1. General Comments

The role of FMEA in IAA was specified in section 3.4. FMEA is a qualitative approach to be used in analyzing system failure. It is referenced in AC 25.1309-1 as a viable tool for both independent failure analysis and as an adjunct to a top-down tool, such as fault tree analysis.

AC 25.1309-1 defines FMEA as "an inductive bottom-up analysis which determines what happens to a system upon single failures of its individual parts." If the item being analyzed is a piece-part of a larger system, these identified failure modes will become the bottom events of a top-down analysis, such as fault tree analysis.

When using FMEA, all potential failure modes of a piece-part are identified. Each mode is then studied, and its impact on system performance is determined. This may be accomplished either empirically or by studying logic diagrams. The empirical approach may involve a technique such as fault insertion. Probabilities must be assigned for each of the failure modes. The development of these failure probabilities may involve some of the techniques discussed in section 7. MIL-STD-1629A is the best guidance document for FMEA.

The preceding paragraph defines the context in which FMEA was applied to RDFCS. Figures 4.2-7 and 4.2-8 depicted the subevents for two events related to the failure of Circuit Cards A13 and A14 in FCC #1. A number of these subevents dealt with microprocessor failure. Since the processor is a general purpose device, continuing the fault tree analysis, which is function oriented, was not desirable. An FMEA was performed instead.

In conducting the pin-level FMEA analysis of a processor, three factors were found to greatly reduce the effort. The first factor is that propagation of most faults under all conditions does not have to be considered. A single effect can usually be found which will totally debilitate the processor. For example, a faulted processor output pin will result in the processor trying to read about half of the data and machine level instructions from the wrong memory addresses. This will result in the coil current comparators tripping, sensor comparisons failing, and in the case of the RDFCS, the iteration monitor failing. In a system using checksums to monitor program memory integrity, these tests will fail.

The second factor which reduces the effort is that many pairs of faults will have the same effect. There are numerous instances of an output pin on one IC being connected only to one other pin. If either pin fails to open, the effect will be the same. Similarly, a ground fault in either pin will produce the same effect.

The third factor which reduces the effort is that there are many instances in which three pins are connected so that one output pin drives two input pins on different circuits. An open fault at each of the input pins can be evaluated first. An open fault at the output pin is then equivalent to both input pins failing open simultaneously. In most cases the effect is the "sum" of the effects of the input pins failing to open; that is, both effects occur. If both input pins are on the same chip, the effect of both being open is more likely to differ from the sum of the individual effects. See figure 5.1-1.

The effect of any of the three pins failing shorted-to-ground is the same in either of the two cases of figure 5.1-1.

Another frequently encountered condition involving three pins is two outputs connected to a single input (figure 5.1-2). In such a case, chips A and B will have three-state outputs, and one or both outputs should be in the high-impedance state at all times. An open fault on the output pin of chip A will then only affect chip C when A has its output enabled. Similarly, an open fault on the output pin of chip B will only affect chip C when B has its output enabled. An open fault on the chip C input pin will usually produce the sum of the effects of open faults on the two output pins. A ground fault on any of the three pins will have the same effect.

Still referring to figure 5.1-2, if a fault should occur, which results in both enable pins being in the enable state, there is a possibility of damage to the A or B chip. If one output is high and the other low, there could be a low impedence path to ground, through the output pins, which could burn out the A or B chip. This depends on the technology used in the individual chips. Frequently, the effect of the original ground fault can be judged to be a total processor failure whether or not the secondary damage occurs.

## 5.2. Application of FMEA to RDFCS

In the RDFCS analysis, three modules of the processor (figure 5.2-1) were considered at pin level.

- The instruction mapper Programmable Read-Only Memory (PROM), which consists of three PROM chips in parallel.
- The microprogram sequencer, which consists of three 2911 sequencer chips in parallel.
- The microprocessor module, which consists of four 2901A chips in parallel.

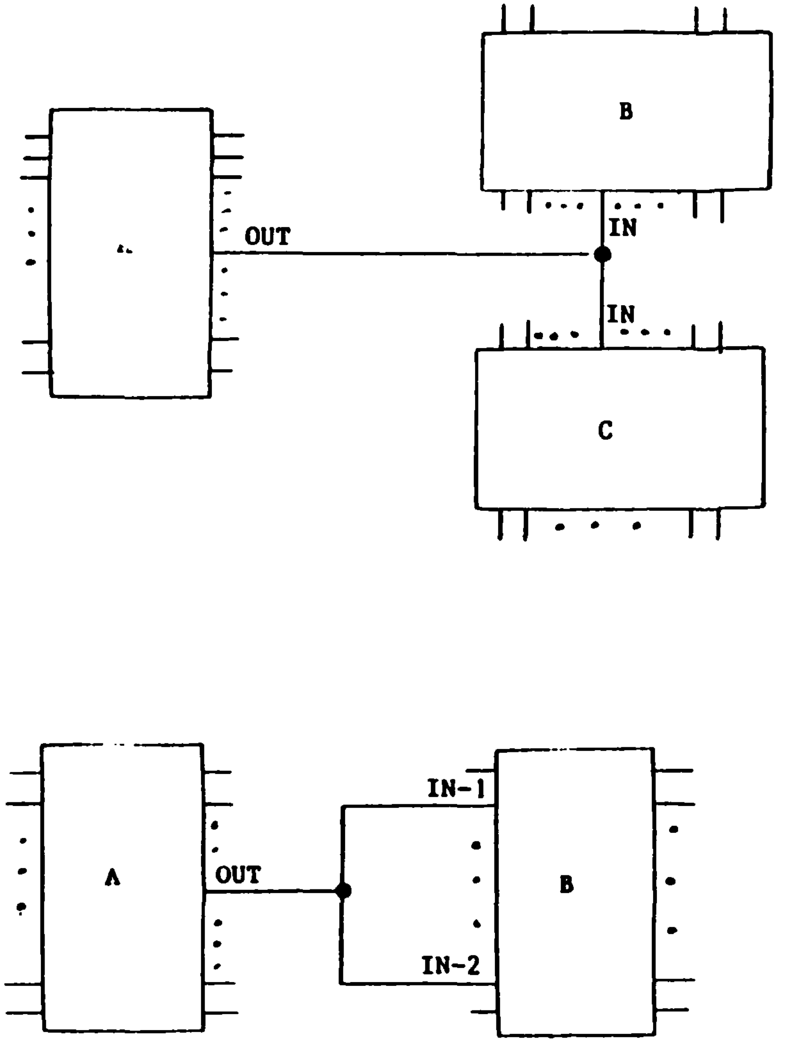
The instruction mapper PROM chips are read-only memory chips. There are two inputs to the chip: machine-level operation codes, and the depth of the stack maintained in the 2901 microprocessors. These are connected to the address pins of the mapper. The data stored in the PROM is the control store PROM address of the first microcode instruction required to execute the machine level instruction with the processor stack at a particular depth. The mapper output pins are only active at the beginning of a microcode sequence, at which time a chip enable signal is sent to the mapper from the next address control PROM.

The microcode address from the mapper PROM is routed to the microprogram sequencer module. This module generates a sequence of microcode addresses, beginning with the starting address from the mapper PROM. Some microcode routines involve jumps to a new address rather than sequential progression only. In such cases, the microprogram sequencer receives the jump address from the control store PROMs and resumes sequential generation of addresses.

The microprocessor module is composed of four 2901A microprocessor chips. Each chip has a word size of four bits, so that the four chips in parallel are used to provide the processor 16-bit word size. This requires that carry signals be passed between 2901As during arithmetic operations. Other interconnections between 2901As are used for data shift operations. The 2901As are controlled primarily by control signals from the control store PROMs in conjunction with the outputs from various registers.

The FMEA, summarized in table C-1 (appendix C), considered three types of pin-level faults: open, grounded, and shorted-to-supply voltage. In most cases, the effect of a fault can be assessed by using the chip logic diagrams, a description of chip/module functions, and the schematic diagrams. The schematic diagrams are reproduced in appendix D.

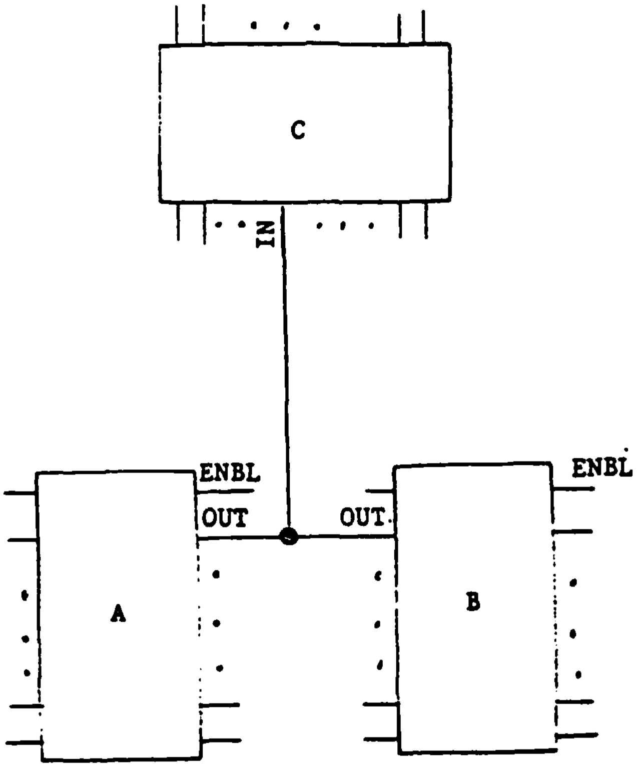
The effect of certain pin faults cannot be determined by analysis using just the above information. In particular, the contents of specific PROM addresses was required or the machine-level code was needed along with the microcode sequences and addresses. Alternatively, the faults could be inserted and the effects observed. The Fault Insertion Approach was taken in this analysis. The results are presented in section 6. For example, it was known that failure of one of the processor pins, used in data shifts (R0, R3, Q0, or Q3 stuck high or low), would result in an immediate disconnect if certain integer words made up of packed Boolean variables were shifted. It was determined from the available information that such shifts might occur, but it was not definite. Similarly, if certain fixed-point numbers were shifted during computation, the commands to the servos would be in error, and the coil current comparators would trip. While both left and right shifts are normally used in multiplication algorithms, it could not be determined that a stuck shift bit would definitely cause such a trip. When the faults were actually inserted, the processor stopped immediately. ("Immediately," as viewed by the human observers.) In this way, fault insertion confirmed the overall effect, a massive processor failure and disengagement of the servos. The exact mechanism by which it occurred was not determined.



EFFECT OF OUTPUT OPEN ON "A" USUALLY SAME AS EFFECT OF INPUT ON "B" OPEN PLUS EFFECT OF INPUT ON "C" OPEN.

EFFECT OF OUTPUT OPEN ON "A" OFTEN NOT SAME AS EFFECT OF IN-1 PLUS EFFECT OF IN-2.

FIGURE 5.1-1. ONE OUTPUT, TWO INPUT CONDITIONS



BOTH "A" AND "B" ENABLED SIMULTANEOUSLY MAY DAMAGE CHIP.

FIGURE 5.1-2. TWO OUTPUT, ONE INPUT CONDITION

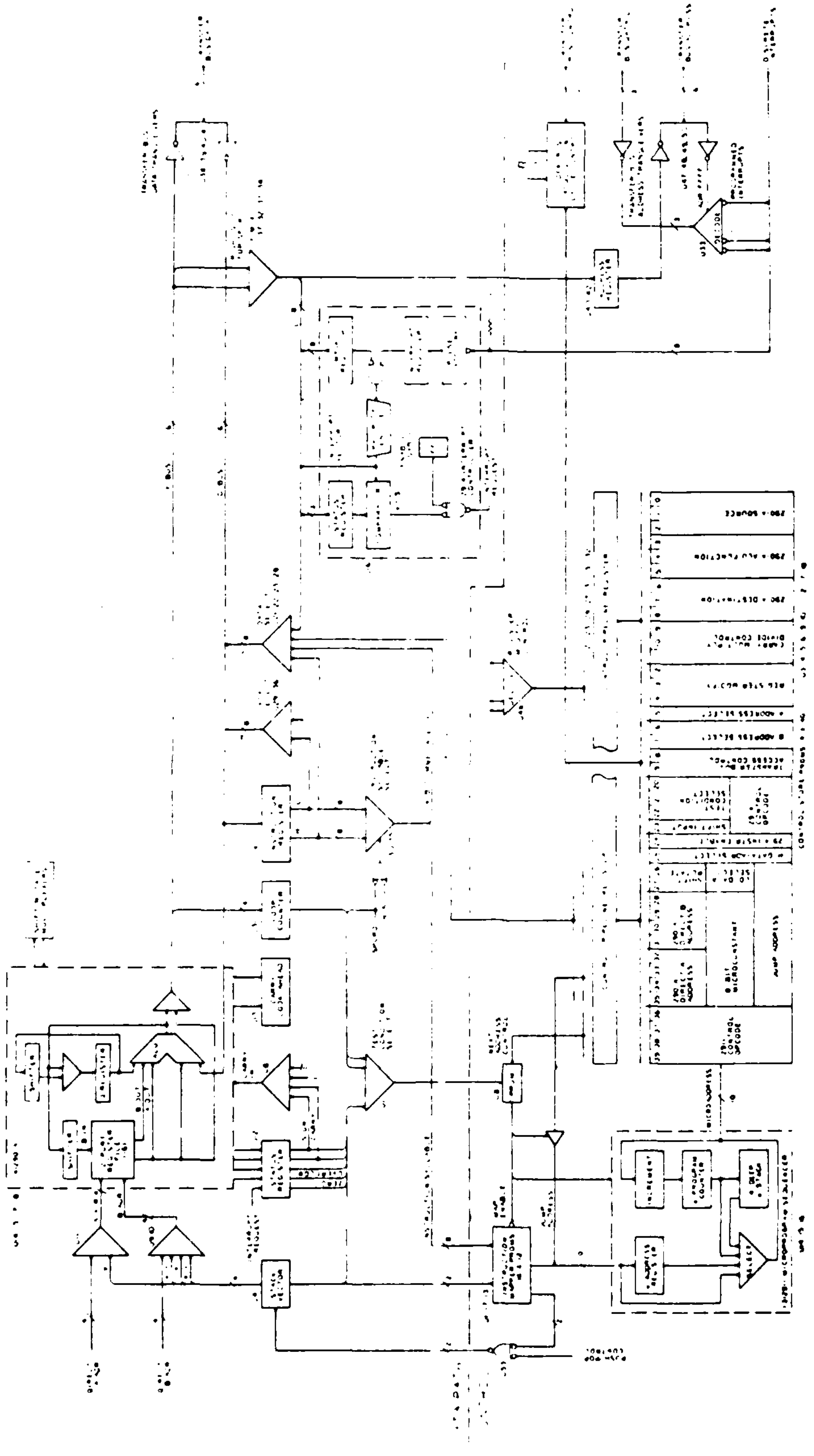


FIGURE 5.2-1. PROCESSOR BLOCK DIAGRAM

# 6. FAULT INSERTION

## 6.1. General Comments

The role of fault insertion in IAA was specified in section 3.5. This technique is required whenever the effect of certain pin faults cannot be determined analytically. The effect of the fault is determined by observing it. Fault insertion may also be used to confirm the effect of faults diagnosed analytically. Another use of fault insertion is to verify fault detection and annunciation systems. In the RDFCS analysis the technique was used for all three purposes.

## 6.2. Application of Fault Insertion to RDFCS

The RDFCS simulator at NASA-Ames was used to insert the faults shown in table E-1 (appendix E). The faults were of two general types: component level faults and IC pin faults. The component level faults were inserted using the FCC breakout panels (figure 6.2-1), the SSP (figure 6.2-2), and the MDICU. Single-sensor faults are those numbered 1 through 19 in table E-1 (appendix E).

Faults representing a dead sensor or a broken wire from the sensor to the FCC were inserted by pulling the appropriate jumper plug at the break-out panel. Faults representing missing sensor validity discretes were also inserted in this way, although they can also be inserted via the DSP (figure 6.2-3). Sensor hardovers and ramps were inserted using the MDICU. Servo faults were inserted using the SSP.

For monitoring the processor detection of sensor faults, the CTAs were used. One of the CTA address windows was set to the address of the Executive Failure (Status) Word (EFW) in each computer channel. The EFW is a 16-bit word with each bit representing a discrete piece of information. There is one EFW for each sensor type in each computer channel. The four low-order bits (0-3) represent, respectively, Executive Failure of My A (EFMA), My B (EFMB), Other A (EFOA), and Other B (EFOB) sensor signals. The data window of the CTA shows the status of the EFW as four hexadecimal characters, with the right-most character representing the bits of interest, 0-3.

The effect of a sensor signal being detected as bad by the software sensor monitor is that certain bits are changed from 0 to 1. With no failures detected, EFMA, EFMB, EFOA, and EFOB are all 0, which is represented in hexadecimal notation as 0. (0000 binary = 0 hexadecimal). When the number 1 sensor of a triple sensor complement is detected to have failed, bit 0 (EFMA) is set to 1 in both channels of FCC No. 1. Bit 1 is also set to 1 so that the comparison monitoring will work properly on the two remaining sensors. The EFW low-order bits will then be 0011, which is 3 in hexa- decimal. The net effect, then, of the number 1 sensor of a triple-sensor set failing is that the value displayed in the CTA window changes from 0000 to 0003. The left three

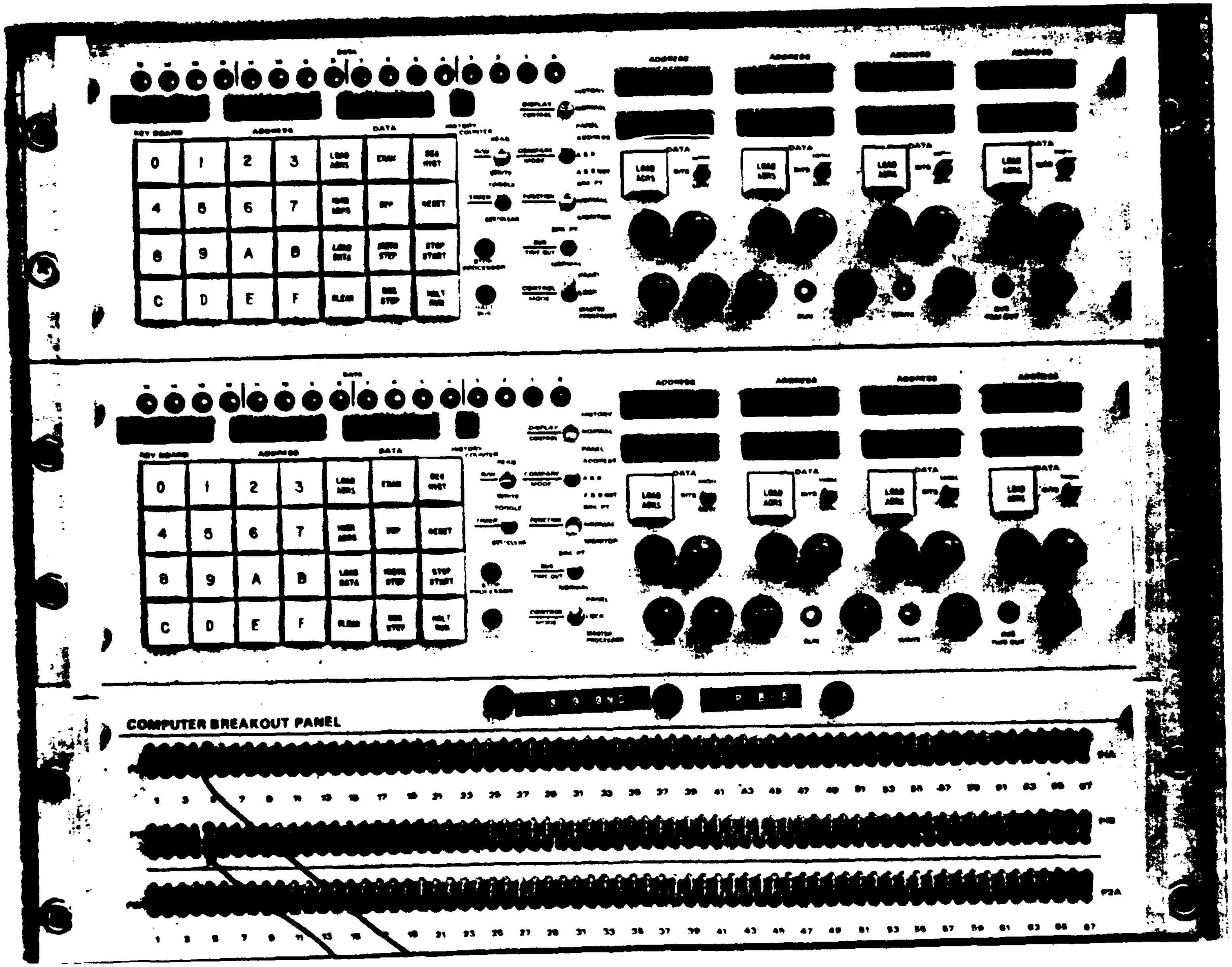


FIGURE 6.2-1. CTA AND COMPUTER BREAKOUT PANEL

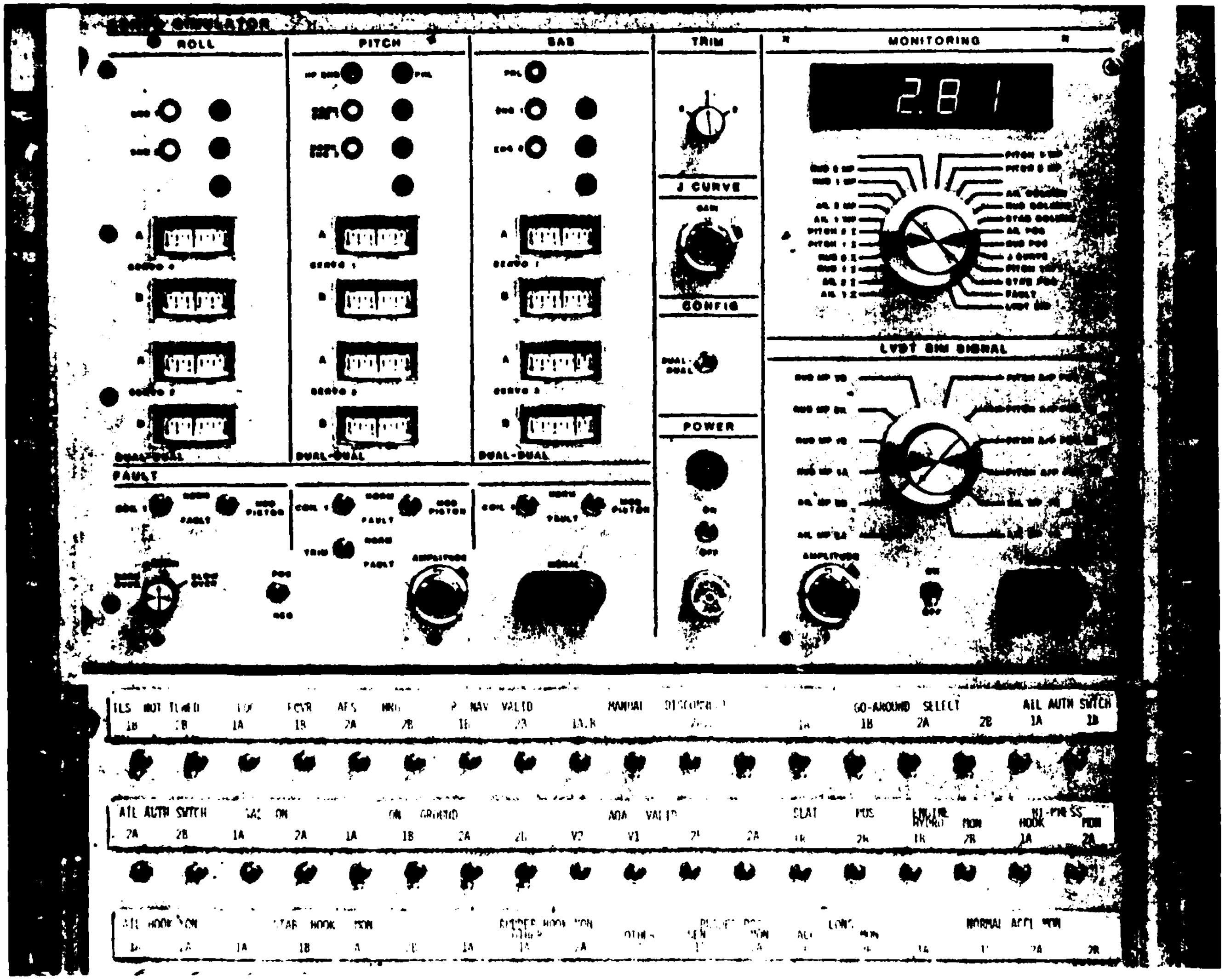


FIGURE 6.2-2. SERVO SIMULATOR PANEL

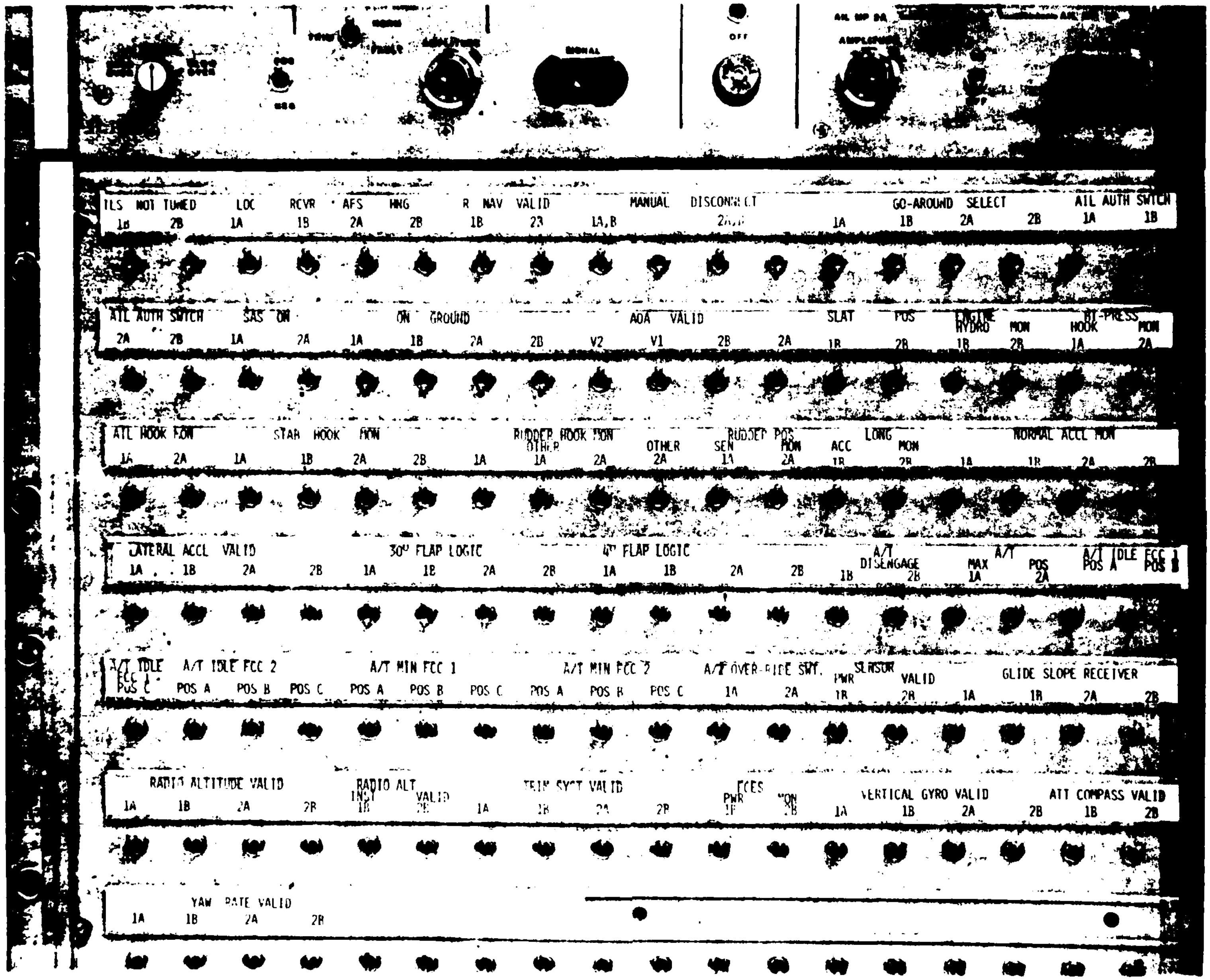


FIGURE 6.2-3. DISCRETE SWITCH PANEL

hexadecimal digits each remains at 0, since each of the corresponding binary bits (4-15) of the EFW remains at 0.

Fault cases 1 through 8 were used to show that the software sensor monitor subroutine is implemented correctly in the RDFCS by subjecting it to a number of different faults in the same sensor type. These cases were also used to show that the results of the sensor monitoring are accounted for in the implementation of the NO DUAL equation, which is also in software. Cases 9 through 16 were then used to show that the voter is involved for various sensor types. Rigorous validation of the system by testing would require that faults be inserted for all sensor types used in automatic landing. In this analysis, performed for illustrative purposes, the full complement of sensor types was not faulted.

In case 2E, NO DUAL did not annunciate even though the fault was inserted with the airplane inbound to the ILS beam intercept point. It is believed to be the result of the inbound leg being flown at an unrealistically low altitude, so that the airplane did not track the glideslope beam for 25 seconds before passing through a 150 ft altitude. A review of the NO DUAL annunciation logic shows that this is the most likely cause, since AP. ONEFAIL was set to true. Low approaches (1500 ft) were being simulated in the interest of time. Approach altitude was subsequently raised to 2000 ft.

Faults 17 through 19 were used to confirm the servo monitoring and the tie-in of the servo monitor outputs to the NO DUAL and disconnect logic. The servo monitors, in particular the coil current comparators, are quite important in ensuring that the airplane does not enter the crucial phase with a faulty computer or servo.

Fault cases 43 through 45 were used to confirm that the FCCs will both disengage upon loss of the second sensor, with the AP.DISC warning displayed, in accordance with the system description.

At the IC pin level, a number of open and ground faults were inserted to confirm the FMEA results of section 6. For this activity, one of the FCCs was removed from the pallet, and the card containing the chip to be faulted was extended for access as shown in figure 6.2-4.

Open pin faults, Cases 20 through 23, were inserted by using multiple sockets between the chip and the circuit card, with a jumper wire replacing the normal pin-to-socket connection. Each fault was inserted by physically pulling the jumper to open the connection. This is a slow procedure, since the chip must be removed and the jumper wire rigged on the desired pin.

The chip and sockets must then be installed and the processors brought back up. This method of inserting open pin faults is only marginally satisfactory. It would be much easier to do if a stack of five or six sockets could be used between the chip and the circuit card. However, the processor will not come up with more than three sockets stacked. The longer electrical paths resulting from the use of the extender card apparently come close to exhausting the avail-

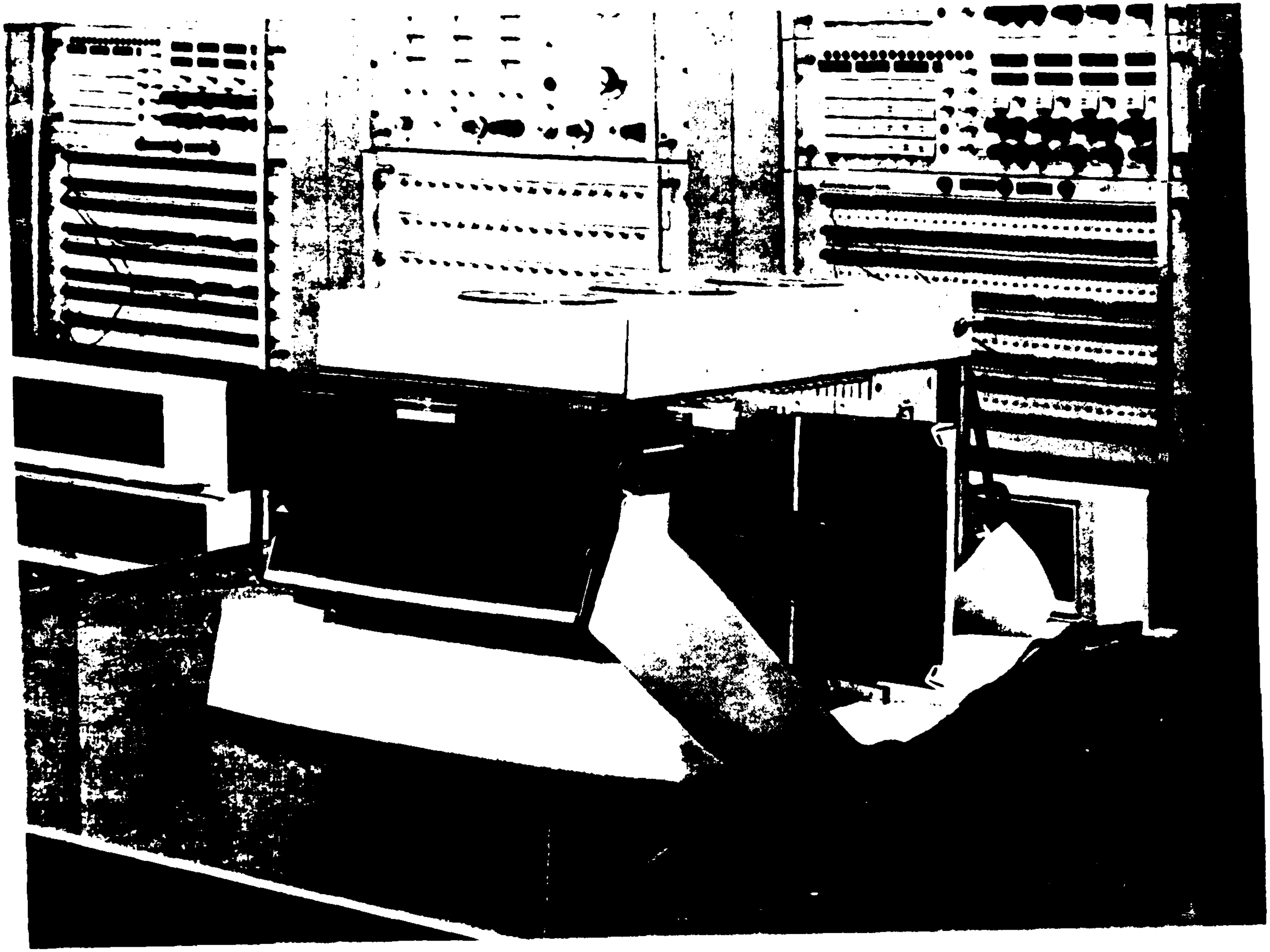


FIGURE 6.2-4. FCC WITH FLIGHT CARD EXTENDED

able tolerance in the timing of the individual microsteps, and the extra path length and capacitance caused by more than three sockets disables the processor.

Grounded pin faults are much easier to insert, since the chip does not have to be removed to set up each case. The processor does have to be brought back up each time, but this is a fairly rapid step. Before each fault was inserted, the data sheets from the chip manufacturer were reviewed (along with the card schematics) to determine that the fault would not damage any chips. No chips were damaged by the ground faults. The ground pin faults are cases 24 through 42 in table E-1.

The chip pin faults all disabled the processor, with the exception of open pin fault 21. This fault involves a pin of a quad 2-input NOR gate. The fault had no effect on the processor operation.

## 6.3. Fault Insertion Results

The faults inserted in the RDFCS simulator achieved the desired results in the assurance assessment of this analysis. More importantly, this confirmed that fault insertion is capable of providing the results required in the IAA. Specifically, the faults inserted confirmed (1) that the NO DUAL warning appears when it should, (2) that all sensor types faulted and required for automatic landing are monitored, (3) that the servo monitoring functions correctly, (4) that the effect of pin-level faults in the processor is in agreement with the FMEA, and (5) that fault insertion is a reasonable way of resolving uncertainty of the effect of open and grounded pin faults in digital hardware. While these results were obtained on a particular system, the approach is judged to be viable for validating other digital systems.

# 7. FAILURE RATE DEVELOPMENT

## 7.1. General Comments

While the development of failure rates is not a safety analysis technique, it is a task that is fundamental to the generation of system probability of failure. In order that fault tree analysis or a statistical prediction tool be able to produce a measure of reliability, individual failure rates must be known. This section discusses the different sources that were used for obtaining failure rates for the RDFCS analysis. The event trees used in the fault tree analysis in section 4 reference these failure rates; they were used in the failure probability computation. Likewise, the rates will be referenced in the reliability analysis found in section 8.

## 7.2. Rationale for Developing Failure Rates for RDFCS

The failure rates for servos, sensors, and indicators were taken from the database maintained by the Lockheed-Georgia Company Reliability Engineering Department. They are composite values for representative components of comparable complexity and construction.

The failure rates for the ICs of the Data Path and Control Cards were estimated using the formulas and tables of *Military Standardization Handbook 217C*. The formulas provide a means of accounting for a significant number of factors:

- Device technology
- Device complexity
- Junction temperature
- Package technology
- Application environment (voltage)
- Usage environment
- Quality level

For example, the equation for the failure rate of a monolithic bipolar device is:

$$f - K_0 \; [C_1 K_T K_V + (C_2 + C_3) \; K_E] \; K_L$$

Where:

f is the device failure rate

$K_O$ is the quality factor

$K_T$ is the temperature adjustment factor for junctions

$K_V$ is the voltage derating stress factor

$K_E$ is the application environment factor

$C_1$ and $C_2$ are complexity factors based on transistor count

$C_3$ is a complexity factor based on package technology and number of pins

$K_L$ is a learning factor

The quality factor, $K_0$, has a value of 1 for devices procured in full accordance with MIL-M-38510, Class B requirements. This value was used for all circuits in this project. It should be noted that the quality factor is a direct multiplier, so that the predicted rate is proportional to it. More or less stringent quality factors can therefore greatly influence the prediction for any individual circuit, circuit board, or entire component.

Junction temperatures are used in determining the adjustment factors $K_T$. The junction temperature is ambient temperature plus the differential resulting from power dissipation through the case. An ambient of 60° was used, with the power dissipation taken from the circuit specification.

The voltage derating stress factor is 1 for the bipolar circuits used in the CAPS processor. The application environment factor is 3.5 for the airborne, inhabited, transport environment of the aircraft underdeck avionic rack. Failure rates for the circuit cards of the FCCs were obtained by summing the failure rates for the card and its components. Table 7.2-1 summarizes the failure rate prediction for the A13 control card. Failure rates for the other cards are shown in table 7.2-2.

Table 7.2-3 presents failure rates for the system components other than the FCCs.

In using these rates in the fault tree and CARSRA analyses, an adjustment was frequently required to include only a portion of the rate, since only certain failure modes are of interest. For example, each dual current comparator has a predicted failure rate of 0.03. Each half of the comparator is given a rate of .01 for the failure mode of failing to trip when the threshold difference is exceeded. This is a very conservative rate for this mode.

TABLE 7.2-1. FCC CONTROL CARD FAILURE RATE

| ITEM | FAILURE RATE* |
|---|---|
| Integrated circuits | 1.788 |
| Resistors | .0018 |
| Capacitors | .224 |
| Oscillator | .25 |
| Coil | .0007 |
| Circuit Board | .023 |
| Edge Connector | .16 |
| Control Card Total | 2.45 |

* All failure rates in failures per million hours.

TABLE 7.2-2. PREDICTED FCC CARD FAILURE RATES

| CARD NO. | FAILURE RATE* |
|---|---|
| A1 Power Supply Monitor | 0.555 |
| A2-A5 PROM Card | .809 each |
| A6 Power Supply Monitor | .55 |
| A7-A10 PROM Card | .809 each |
| A11 Terminator/Test Access | .555 |
| A12 RAM Memory Control | 1.18 |
| A13 CAPS Control | 2.45 |
| A14 CAPS Data Path | 1.98 |
| A16 Cross-Channel Receiver | .70 |
| A17 DITS Transmitter | 1.75 |
| A18 D/A Servo Command | 1.75 |
| A19 Terminator/Time Synch | 1.40 |
| A20 Discrete Output | 2.79 |
| A21 Data Transmitter/Receiver | .70 |
| A22 Serial Digital Input No. 1 | 1.65 |
| A23 Serial Digital Input No. 2 | 1.80 |
| A24 Autoland Sensor Input | 1.80 |
| A25 Cruise Sensor Input | 1.12 |
| A26 Data Acquisition | 1.20 |
| A27 Discrete Input | 1.30 |
| A28 Servo Engage Logic | 2.61 |
| A29 Cross Channel XMTR | 1.20 |
| A30-A32 Servo Amplifier | 3.00 |
| A33 Speed Servo Amp | 1.70 |
| A300 Speed Command XMTR | 1.70 |
| A400 Power Supply | 21.0 |
| A500 Power Supply | 21.0 |

* All failure rates in failures per million hours

TABLE 7.2-3. FAILURE RATES FOR MAJOR RDFCS COMPONENTS

| COMPONENT | UNIT FAILURE RATE* |
|---|---|
| Pitch Angle Gyro | 303 |
| Roll Angle Gyro | 303 |
| Yaw Rate Gyro | 200 |
| Accelerometer | 74 |
| Radio Altimeter | 756 |
| ILS Receiver | 252 |
| Air Data System | 167 |
| Roll Autopilot Servo | 14 |
| Pitch Autopilot Servo | 15 |
| Yaw Autopilot Servo | 14 |
| EH Valve Drive Coil | 1.0 |
| LVDT | .72 |
| Dual Current Comparator (Hardware) | .03 |
| Warning Annunciator (per function) | 8.3 |

* These are not actual failure rates for any particular airplane or for any single component produced by a particular manufacturer. They are representative rates determined by a review of generic component types on a number of airplane models in a variety of commercial and military applications. All failure rates in failures per million hours.

# 8. RELIABILITY PREDICTION USING CARSRA

## 8.1. General Comments

AC 25.1309-1 emphasizes the need for probability analysis in determining system reliability. This circular defines reliability to be "the probability that a system, subsystem, unit or part will perform its intended function for a specified interval under stated operational and environmental conditions." The following three probability classifications are specified:

- Probable: Probable events may be expected to occur several times during the operational life of each airplane. A probable event has an occurance probability on the order of 1.0 x $10^{-5}$ or greater.

- Improbable: Improbable events are not expected to occur during the total operational life of a random single airplane of a particular type, but may occur during the total operational life of all airplanes of a particular type. An improbable event has a probability on the order of 1.0 x $10^{-5}$ or less.

- Extremely Improbable: Extremely improbable events are so unlikely that they need not be considered to ever occur, unless engineering judgment would require their consideration. An extremely improbable event has a probability on the order of 1.0 x $10^{-9}$ or less.

Aircraft functions fall into three categories: Non-essential, Essential, and Critical. Section 3.1 discusses these three categories; AC 25.1309-1 provides a better discussion. Errors in a non-essential function may be probable. Errors in an essential function must be improbable. Errors in a critical function must be extremely improbable.

An IAA is performed on a particular aircraft system performing a function, e.g., the RDFCS. The RDFCS becomes a critical system when the airplane is executing an automatic landing, during the last 150 ft of descent.

## 8.2. RDFCS Reliability - Fault Tree Analysis

As demonstrated in section 4.3, the probability of system failure may be computed from the fault tree analysis. The two scenarios that could result in the aircraft's improperly accomplishing or losing the critical function performed by the RDFCS had a combined probability of 0.638 x $10^{-9}$. A third scenario, that conditions encountered are outside the system design requirements or control laws are deficient, was not considered (see section 4.2). The probability of failure of the RDFCS is "extremely improbable." The concern is that an error was made producing a low system failure probability and that the error remains undetected. An independent confirmation of this reliability is needed.

## 8.3. RDFCS Reliability - CARSRA

CARSRA is an analytical reliability prediction program used in this IAA to obtain the probability of system failure (Bjurman, et al., 1976). In this analysis, the probability of failure is only considered during the crucial flight phase, which has a duration of 0.02 hours. Although CARSRA was used in this assessment, some other method (except fault tree analysis) could be used for the verification. These alternatives were discussed in section 3.5.

## 8.4. CARSRA Application

CARSRA is an application of stochastic processes. Stochastic processes concern sequences of events governed by probabilistic laws. Applications exist in many physical and social sciences, as well as engineering. The explosion of system failure into its elemental causes with probabilistic relationships (fault tree analysis) suggests that viewing the error tree as a stochastic process may be an aid in analysis. The reader need not have a strong statistical background in order to understand this discussion. There are a large number of possible references on stochastic processes. Karlin (1966) was used in the preparation of this tutorial.

### 8.4.1. Configuration Description

The CARSRA computer program requires that the user provide an input description of the system under analysis. Three levels of organization are implicit in the CARSRA inputs; the user must adhere to these levels. At the top level is the system, in this case the RDFCS. System failure probabilities constitute the primary output provided by CARSRA. The intermediate level is comprised of stages. Each stage consists of one or more identical modules, which are at the lowest level. In the RDFCS, each sensor is a module, and like sensors form stages. For example, each of the three Normal Accelerometers (NA) is a module and the three NA together comprise a stage. CARSRA determines system reliability as a function of time; the success of the system is based on dependencies between stages, functional redundancy, and module redundancy.

### 8.4.2. Markov Models

A Markov process is a type of stochastic process. Chapter 1.3 of Karlin (1966) contains a mathematical definition of both stochastic and Markov processes. A Markov model is a Markov process used to describe a particular system or subsystem. Markov models were selected by the CARSRA developers as a major part of the program's analytical framework. The following discussion of these models includes some material on applying CARSRA to systems other than the RDFCS. This material is intended to benefit readers not familiar with the rationale of developing the input parameters for Markov models as used in CARSRA.

A Markov model is used to describe the number of failed and operating modules within each stage. The transition rates from state to state are used by CARSRA in computing state occupancy probabilities. A separate Markov model is used for each stage. State 1 is the no-failure state in each model, and the two states with the highest numbers correspond to stage failure. The Model always starts in State 1. For example, a dual stage (one of two identical modules required for the stage to function) might have four states, as shown in figure 8.4-1. State 1 represents both modules working. State 2 represents one module failed and one working. States 3 and 4 represent both modules failed. The highest numbered state (state 4 in this case) represents undetected stage failure, while State 3 represents detected failure. Note that State 2 does not distinguish which module has failed.

State transition rates must be supplied to CARSRA by the user. These are generally functions of the module failure rates, and possibly other parameters. Returning to the example of the dual stage used previously, the Markov state diagram would be as in figure 8.4-1. Transition rate $f_{12}$ is the rate at which transitions occur from State 1 to State 2. That is, if the system is in State 1, the probability that it will transition to State 2 during a short increment of time, dt is $f_{12}dt$. The other transition rates are similarly defined.

If there is no monitoring or switching required when the first module fails, and if there is no possibility of the stage failing undetected, the transition from State 1 will always be to State 2, and the transition from State 2 will always be to State 3. Transition rate $f_{12}$ will be simply 2f, and $f_{23}$ will be f, where f is the failure rate of a single module. The other transition rates will be 0. Note that this means that State 4 will never be occupied, consistent with undetected stage failure being impossible.

In many instances encountered in real systems, digital or otherwise, a reconfiguration must occur before the redundancy can be determined. In the example dual case, an output monitor could be used on each module. If the monitor can detect 97 percent of module failures, e.g. no output or unreasonable output, the monitor provides "coverage", c, of 97 percent. The transition rate $f_{12}$ is then 2fc, so that 97 percent of the transitions from State 1 go to State 2.

Of the remaining three percent of the transitions from State 1, some fraction, e.g., 2/3, could go to State 3 and the rest to State 4. This would result in $f_{13}$ being 2f(1-c)(2/3) or 2f(.02), and $f_{14}$ being 2f(1-c)(1/3) or 2f(.01).

Note the distinctions between coverage (which relates to module failure detection) and undetected stage failure. Note also that the function of a particular stage could be such that it cannot fail undetected, even though individual modules within the stage may fail with coverage less than 1. In other cases, stage failure may be detected only by multiple module failures being detected.

The sum of transition rates out of State 1 is 2f. In general, if any state corresponds to N modules working, the sum of transition rates out of that state will be Nf.

Stages can fail for two reasons: spares exhaustion or coverage failure. In contemporary aircraft systems having critical functions to perform, coverage failures are of as much concern as spares exhaustion.

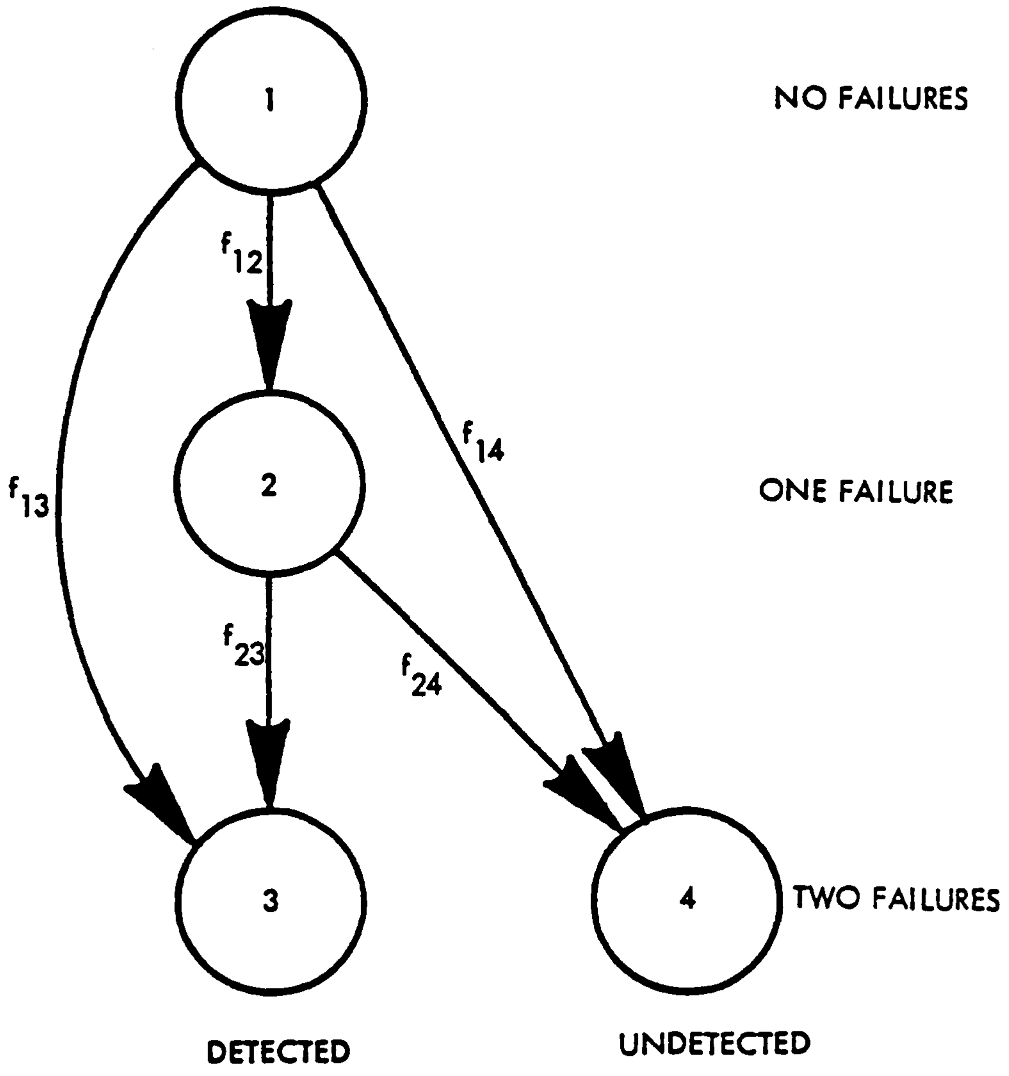


FIGURE 8.4-1. MARKOV MODEL OF DUAL STAGE

In the previous dual stage example with 97 percent coverage of the first module failure, no consideration of the failure rate of the monitor itself was included. The coverage factor of 97 percent means that 97 percent of the module faults are of such a nature that they can be detected by an unfailed monitor. The rest are outside of the monitor's capability. In cases where dedicated hardware monitors are used, it is appropriate to consider their failure rates and failure modes. A two-state monitor is the type most frequently encountered. It provides only a GOOD/BAD signal. Such a monitor has only two failure states: false indication of BAD when the module is good, and false indication of GOOD when the module is bad.

The simplest way of treating such monitors in CARSRA is to combine the monitors with the modules as a single stage. The transition rate from State 1 to State 2 is then

$$2fcr_m + 2f_ma$$

where:

$f$ = the failure rate of a single module
$c$ = the coverage
$r_m$ = the reliability of the monitor over the entire flight time
$f_m$ = the monitor failure rate
$a$ = the fraction of monitor failures resulting in a good module being declared bad.

The other transition rates would be similarly defined, recognizing the relation between detection of stage failure and component monitors. Each instance of such a stage must be evaluated individually in determining the applicable rate formulas.

Frequently, certain terms in a rate equation can be ignored because they are numerically negligible. For example, if $f = 120 \times 10^{-6}$ and $f_m = 0.1 \times 10^{-6}$, the term $2f_ma$ can be ignored in the formula

$$f_{12} = 2fcr_m + 2f_ma$$

provided c is not absurdly small. If c is 90 percent, a is 50 percent, and the flight time is ten hours,

$$f_{12} = 2(120 \times 10^{-6})(.90) \exp(-.1 \times 10^{-6} \times 10) +2 (.1 \times 10^{-6})(.50)$$

$$= 216 \times 10^{-6} + .1 \times 10^{-6}$$

Inclusion of the term yields a rate of $216.1 \times 10^{-6}$; ignoring it yields $216.0 \times 10^{-6}$. The difference is much less than that caused by uncertainty in the module failure rate, $120 \times 10^{-6}$.

### 8.4.3. Dependencies

CARSRA permits the user to describe instances in which failures of a module in one stage will prevent a module in another stage from being used. An example of this in the RDFCS is the portion of each FCC channel which receives sensor data and makes it available to the other channels. Data Acquisition Card A26 in FCC No. 1 receives data from the No. 1 unit of each triple sensor type and relays it to another card for transmission to the other three channels and for use by its own channel. There are five triple-sensor types involved in the autoland mode: pitch, roll, and yaw-rate gyros, and lateral and NA. (The A26 card also handles data from other sensors, but only these five will be used for discussion here.) If the A26 card fails in FCC No. 1, the data will be lost from pitch gyro No. 1, roll gyro No. 1, yaw-rate gyro No. 1, lateral accelerometer No. 1, and normal accelerometer No. 1, just as if all five of these sensors had failed. The A26 card is called a dependency module and its stage a dependency stage. Each of the affected sensors is called a non-dependency module, and the corresponding stage a non-dependency stage.

Coverage for sensor failures is provided by comparison monitoring and reconfiguration. Each channel independently performs the sensor monitoring functions on the data it will use in control law computations. When an A channel detects a failed sensor, it does not transmit the identity of the individual sensor to the other channels. When a B channel detects a failure, it does transmit a discrete variable, AP.ONEFAIL, to the A channel in the same FCC. The A channel will turn on the NO DUAL annunciation based on its receipt of AP.ONEFAIL from B or its own detection of a sensor failure. The NO DUAL indication is provided to inform the crew that the RDFCS is not fail-operational. The No. 1 FCC drives the No. 1 Warning Annunciation Indicator (WAI) and the No. 2 FCC drives the No. 2 WAI, so that warning will be provided if either channel of either FCC detects the failure.

The sensor monitoring is part of the foreground flight software. Consequently, for a channel to detect a fault, the CAPS processor must function, as must the CAPS bus and portions of the program and data memory. These are the same hardware elements which perform other functions, such as control law computations and mode logic computations. Most faults in these circuits will result in a totally debilitated processor, so that the inability to the monitor sensors is inconsequential. Note also that even if one channel does lose the ability to monitor sensors, any one of the other three channels can force the NO DUAL warning.

Therefore, the only appreciable probability that the loss of fail-operational sensor capability will not be annunciated results from loss of both WAIS. The multiple-function WAI has a unit failure rate prediction of 33 per million hours. The failure rate of any one of the eight warning messages is conservatively taken to be one-fourth the unit rate, or 8.3 per million. The FCC activates the NO DUAL message by providing a ground to the WAIs, so that a broken wire or bad connector contact would prevent annunciation. A rate of 1.3 per million hours is included for such failures. Also, the Discrete Output (A20) and Servo Engage Logic (A28) cards are involved, with failure rates of 2.79 and 2.61 per million hours, respectively. Even though only a portion of the failures of these cards will affect NO DUAL, the full rate is used. Further analysis could reduce this rate substantially. The failure rate for NO DUAL is then

| | |
|---|---|
| WAI | $8.30 \times 10^{-6}$ |
| Wiring | 1.30 |
| A20 Card | 2.79 |
| A28 Card | 2.61 |
| | $15.00 \times 10^{-6}$ |

The probability of failure in a 4-hour time period is then $60 \times 10^{-6}$. The probability of both NO DUAL warnings being lost is the square of this number, $3.6 \times 10^{-9}$. The test button on the WAI results in the FCC circuitry and the wiring being tested as well as the WAI itself. Thus latent failures are not a problem, provided the indicators are tested prior to autoland.

The factor $3.6 \times 10^{-9}$ is used as the probability that the first failure of a sensor type will not be covered. This does not constitute stage failure, either detected or undetected. Undetected stage failure is assumed to occur on second failure, provided the first failure was undetected. This is somewhat a misuse of the term "undetected"; the stage failure itself is not necessarily undetected, but the increased likelihood of its occurrence, following first failure, is not annunciated.

This treatment of sensor failures allows the availability feature of CARSRA to be used in computing the probability of loss of one sensor prior to 150 ft, failure of the NO DUAL annunciation, and another failure below 150 ft.

8.4.4. Availability

CARSRA permits system reliability to be computed for a mission phase which follows a period of operation with less stringent failure criteria. An obvious example of this is the RDFCS, which is fail-passive in cruise, but must be fail-operational in autoland below 150 ft. The availability feature allows the user to specify which modules may be failed at the beginning of autoland without forcing diversion to an alternate landing site. Each such availability configuration must provide adequate reliability for the landing, although not as much as if everything is working. The RDFCS requires all of the modules used in autoland to be operational, so that the availability feature might seem not needed in this assessment. It is needed, though, to compensate for a capability which CARSRA lacks.

The reliability of the RDFCS for automatic landing is predicated on the system being fail-operational as the alert height is passed. Therefore, the probability of the system having a latent failure at 150 ft and a second failure below that point must be quite small.

By setting up the CARSRA input to allow one sensor of each type to fail during cruise, with the transition rate from State 2 to the undetected failure state including the coverage factor of $3.6 \times 10^{-9}$, the undetected system failure probability computed by CARSRA will give the probability of an undetected latent failure at 150 ft and a second failure before touch-down. (See figure 8.4-2.)

What CARSRA will actually compute is:

$P_1 \times P_2 + P_3 \times P_4$

where,

$P_1$: probability of 0 failures at 4 hours

$P_2$: probability of undetected failure and detected failure between 4 and 4.02 hours

$P_3$: probability of 1 undetected failure at 4 hours

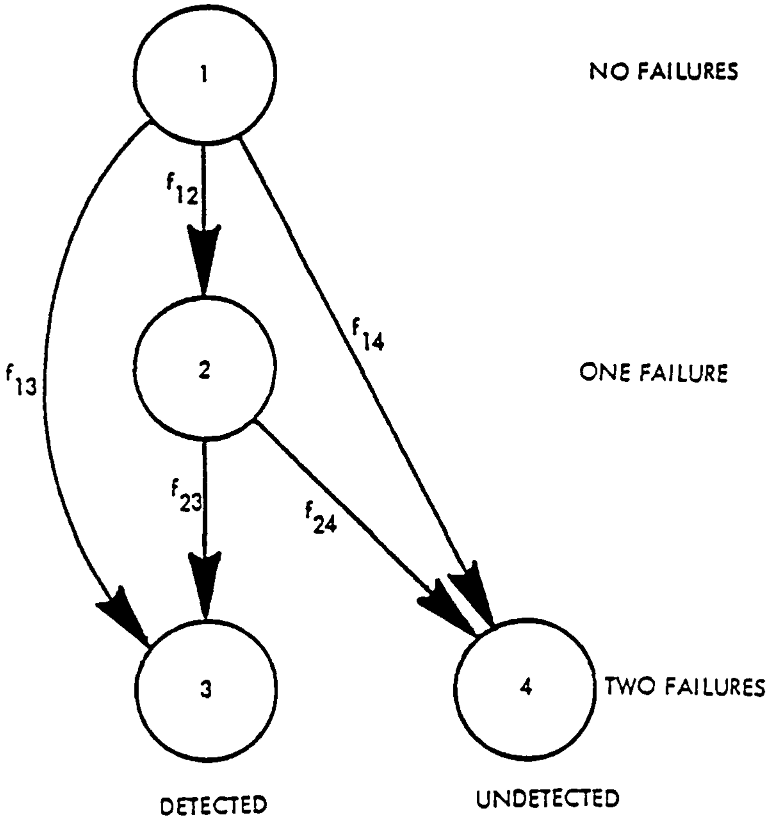
$P_4$: probability of second failure between 4 and 4.02 hours

Since the probability of both an undetected and a detected failure between 4 and 4.02 hours is very small, the first term is negligible and the output will be equal to the second term, which is the probability desired. This approach is used for the undetected (unannunciated) failures throughout the system. The definition of stages and the transition rates are shown in figure 8.4-3.

The CARSRA program is sensitive to the precision of the host computer. During this analysis, some negative probabilities for unannunciated failures were computed. It is suspected that this may have been caused by the 36-bit word length of the Univac 1100-series computer. The transition rates to the unannunciated failure states are quite small, in some cases $1.0 \times 10^{-13}$, and addition/subtraction of numbers of this magnitude with numbers close to 1.0 could produce some numerical accuracy problems on a 36-bit machine. If the program is run on a computer with a 64-bit word length, the problem is thought to be unlikely.

Because of the numerical problem encountered with the CARSRA output, the system failure probabilities reported here were actually manually calculated. This was done by manually computing the stage occupancy probabili-ties, and then combining these probabilities to account for dependencies between stages, using the same logic that the CARSRA program uses.

The probability of an undetected failure prior to the crucial phase, followed by a second failure in the crucial phase, is $3.36 \times 10^{-14}$, compared to $2.46 \times 10^{-14}$ from the fault trees. The probability of multiple failures in the crucial phase, if everything is working just prior to the phase, is $0.658 \times 10^{-9}$, compared with $0.638 \times 10^{-9}$ from the fault trees. These results are shown in table 4.3-1.



| | DUAL SENSOR | TRIPLE SENSOR |
|---|---|---|
| $f_{12}$ | 2f | 3f |
| $f_{13}$ | 0 | 0 |
| $f_{14}$ | 0 | 0 |
| $f_{23}$ | f | 2f |
| $f_{24}$ | fa | 2fa |

f = MODULE FAILURE RATE

a = ANNUNCIATION FACTOR $3.6 \times 10^{-9}$

FIGURE 8.4-2. MARKOV MODEL CODING FOR SENSOR STAGES

RDFCS 1/6

```
        12         9
         1         4         2 A500 PWR. SUP
           42.
                   21.

         2         4         2 A400 PWR. SUP.
           42.
                   21.

         3         5         3 ACP 201 PWR. SUP.
           87.
                   58.
                           29.

         4         4         4  A21/221 CARDS
           2.80
                  2.10  .0000001
                           1.40
         5         4         4  A26/226 CARDS
           4.80
                  3.60  .0000001
                           2.40
         6         4         4  A24/A224 CARDS
           7.20
                  5.40  .0000001
```

FIGURE 8.4-3. CARSRA INPUT (1 of 6)

RDFCS 2/6

```
                           3.60
         7         4         4    A27/227 CARDS
           5.20
                  3.90  .0000001
                           2.60
         8         4         4    A22/23 CARDS
          13.80
                 10.35  .0000001
                           6.90
         9         4         2    PROCESSORS
         116.96
                 58.48  .0000006

        21         4         3    PITCH GYRO
          909.
                  606.  .0000022

        22         4         3    ROLL GYRO
          909.
                  606.  .0000022

        23         4         3    YAW GYRO
          600
                  400.  .0000014

```

FIGURE 8.4-3. CARSRA INPUT (2 of 6)

RDFCS 3/6

```
        24         4         3   NORM. ACCEL.
          222.
                  148.  .0000005

        25         4         3   LAT. ACCEL.
          222
                  148.  .0000005

        26         4         2   RAD. ALT
         1512.
                  756.  .0000007

        27         4         2   LOC. RCVR
          252.
                  126.  .0000005

        28         4         2   GS. RCVR
          252.
                  126.  .0000005

        29         4         2   DADS
          334.
                  167.  .0000001

        30         4         2   ROLL SERVO
```

FIGURE 8.4-3. CARSRA INPUT (3 of 6)

RDFCS 4/6

```
          28.
                  14.  .0000001

        31         4        2   PITCH SERVO
          30.
                  15.  .0000001

        32         4        2    YAW SERVO
         28.
                  14.  .0000001

    4.0       4.0      .02      .02
        27
  11  41  42  51  52  61  62  71  72  81  82  91
  12  43  44  53  54  63  64  73  74  83  84  92
  21 211 221 231 241 251
  22 212 222 232 242 252
  31 211 221 231 241 251
  32 212 222 232 242 252
  33 213 223 233 243 253
  41 211 221 231 241 251 261 271 281 291
  42 261 271 281 291
  43 212 222 232 242 252 262 272 282 292
  44 262 272 282 292
  51 211 221 231 2 1 251 261 271 281 291
```

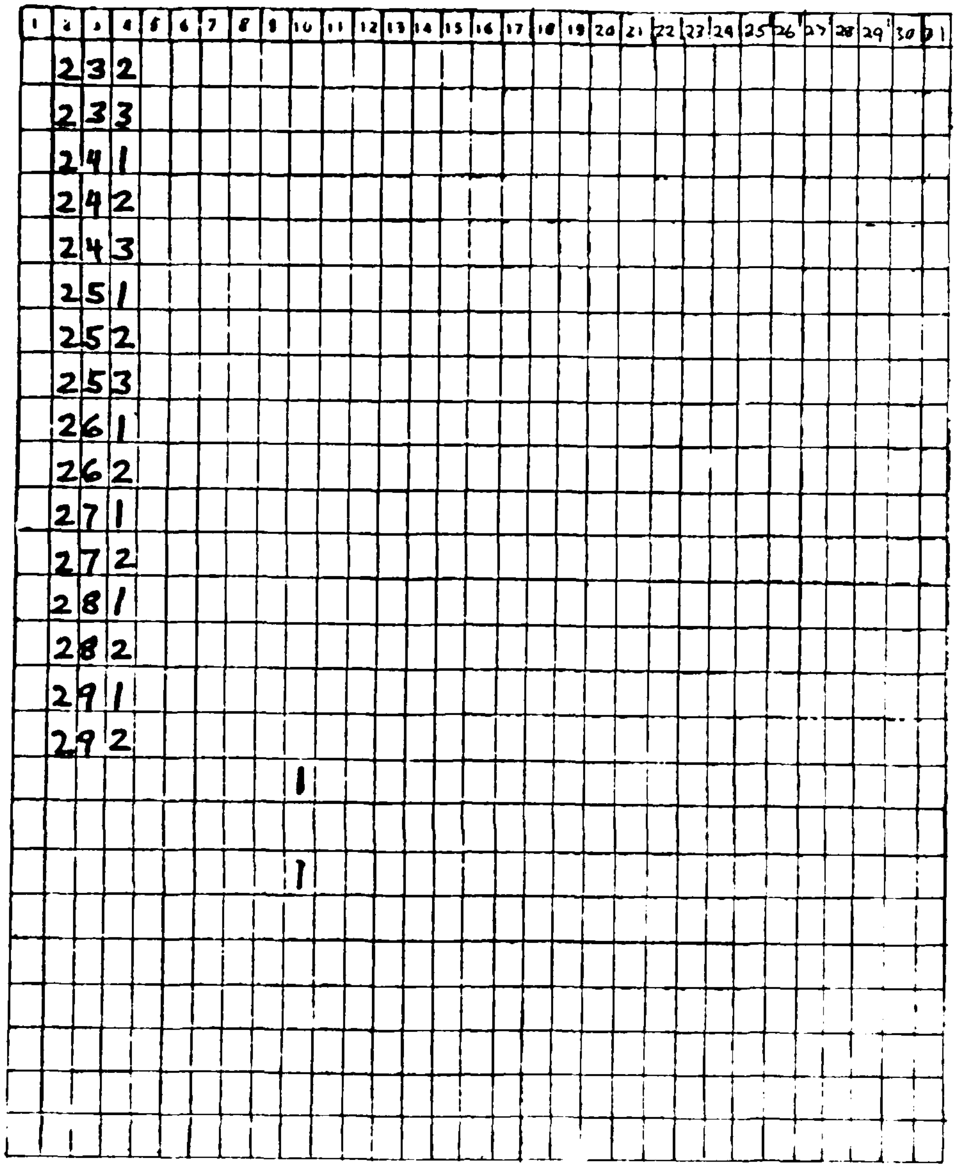
FIGURE 8.4-3. CARSRA INPUT (4 of 6)

RDFCS 5/6

```
  52 261 271 281 291
  53 212 222 232 242 252 262 272 282 292
  54 262 272 282 292
  61 211 221 231 241 251
  63 212 222 232 242 252
  71 211 221 231 241 251 261 271 281 291
  72 261 271 281 291
  73 212 222 232 242 252 262 272 282 292
  74 262 272 282 292
  81 261 271 281 291
  82 261 271 281 291
  83 262 272 282 292
  84 262 272 282 292
  91 301 311 321
  92 302 312 322
        25
  91
  92
 211
 212
 213
 221
 222
 223
 231
```

FIGURE 8.4-3. CARSRA INPUT (5 of 6)

RDFCS 6/6



```
 232
 233
 241
 242
 243
 251
 252
 253
 261
 262
 271
 272
 281
 282
 291
 292
         1

         1
```

FIGURE 8.4-3. CARSRA INPUT (6 of 6)

# 9. SUMMARY

## 9.1. Background

The purpose of this tutorial is to provide certification engineers with a background in IAA. The vehicle for accomplishing this is to provide a walk-through of a system failure analysis using a critical system, the RDFCS. The complexity of airplane systems (RDFCS being a prime example) has necessitated the evolution of safety analysis techniques that permit the diagnosis of failure effects of multiple faults, both intra- and intersystem. A diagnosis of this type is important in demonstrating compliance with Part 25 of the FARs for "flight-essential" and "flight-critical" avionic systems. AC 25.1309-1 provides guidance material for complying with the above regulation. The techniques suggested in the AC were the basis for the RDFCS analysis. The analytical techniques were selected to mutually reinforce each other on the following bases:

- Fault tree analysis identifies the conditions and functional failures contributing to a defined failure condition. It is also used to compute a quantitative assessment of reliability (system failure probability).

- Analytical reliability prediction analysis confirms the system failure probability computed with fault tree analysis.

- FMEA was used to augment fault tree analysis in diagnosis below the circuit card level.

- Fault insertion was used to confirm the fault detection and tolerance capabilities of the RDFCS. The existence of the RDFCS Simulator made fault insertion possible.

The integration of the above techniques was exemplary. The selection of safety analysis techniques for integration is the responsibility of the test/certification engineer and must be customized to the system. The use of any IAA model must supplement, but not replace, the judgment of the FAA certification personnel.

## 9.2. Concluding Remarks

The concluding remarks for this tutorial relate to the benefits and limitations of the IAA model used in the RDFCS analysis. During the course of this analysis, certain enhancements were visualized that would have improved the study. These enhancements will be discussed in section 9.3. They are included in this tutorial, because of their potential application to other integrated analyses.

IAA is workable for a system, such as the RDFCS, which employs monitoring totally separate from the hardware/software being monitored. In the RDFCS, this monitoring includes the servo coil current comparators and the modulator piston followup monitoring. It also includes the warning annunciations which one FCC can generate following a failure in the other FCC. A single-string, self-monitored system might be much less amenable to this approach, depending on the monitoring approach used.

Fault tree analysis is a feasible analytical method for identifying system level faults. One benefit is that specific software failures are identified as the analysis progresses. These can be, and should be, used as a check on the validation test case selection to assure that the software function is rigorously tested. Fault trees can be extended to the circuit card level in a well organized computer such as that used in the RDFCS. In general, the analysis is facilitated by a design with clearly partitioned and identifiable functions, and an interface structure which is consistent for all card inputs and outputs.

FMEA is more easily accomplished than fault trees within the processor itself. This is because the processor is involved in a diverse set of functions defined by the flight software. Most individual pin-level faults have many effects. Usually, each fault can be traced to an effect which totally debilitates the processor. Other effects, which cause massive processor failure or erroneous results only under certain conditions, do not have to be analyzed in detail when their effects do not propagate across channels. In contrast, a fault tree analysis based on loss of required system functions would result in identification of the same hardware faults time after time. When a system simulator exists, fault insertion is an important adjunct to FMEA.

Fault tree analysis and reliability analysis tools, such as, CARSRA, provide comparable results for relatively straightforward redundancy conditions, e.g., the probability of multiple failures during the crucial phase when all components are working at the beginning of the phase. For more complicated situations, the two methods do not agree as closely. This is a result of different simplifications and assumptions being made to structure the problem to the two methods. For example, the third sensor of a triple sensor set (figure 2.1-1) has redundant input paths to the computers (the data input sections of the two computer B channels), but the other sensors have only a single data path (the A channel input sections). This is treated correctly in the fault trees, but the redundancy cannot be accounted for in CARSRA. The conservative assumption is therefore made that loss of either B channel sensor input capability will cause loss of the third sensor in all triple sensor sets. In validation work, any assumptions required can be made conservatively so that the computed failure probability is actually an upper bound on the true probability.

## 9.3. Analysis Enhancements

The RDFCS simulator was invaluable as a tool in the failure analysis function. Given sufficient access to the simulator, the FMEA and fault insertion test sessions should be scheduled on an iterative basis. After performing certain FMEAs, a fault insertion session should be used to confirm the analysis to that point. The results should then be incorporated in the FMEA, and the entire FMEA reviewed in light of those results. This review may lead to identification of additional fault cases which should be simulated to resolve uncertainty which may have arisen. This iterative approach was not used in the subject study because of limitations on the availability of the simulator.

The RDFCS simulator has substantial capability for research investigations of DFCS validation issues. This capability would be significantly improved by an automated fault insertion and data recording capability. Such a capability should be preprogrammable with a list of faults to be inserted. It should include a means of recording the impact of each fault (e.g., changes in the values of discrete variables) for many more variables than the four accessible through the CTAs. It should allow variables in channels other than the faulted one to be accessed and recorded.

Care should be taken in selecting a computer tool for analytic reliability prediction. The nature of the analytical program requires a high degree of numerical precision when solving certain problems. In the subject study (see section 1.2) the system failure probabilities used to confirm the fault tree analysis computations were manually calculated. This was done by manually computing the stage occupancy probabilities and then combining these probabilities to account for dependencies between stages. The logic used was identical to that used by the CARSRA program. The problem was thought to be due to the small failure rates and the accompanying precision difficulties encountered on a computer with a 36-bit word length. If so, the use of CARSRA on a computer with a 64-bit word length would have remedied the problem.

# APPENDIX A - SUMMARY DESCRIPTION FOR REDUNDANT DIGITAL FLIGHT CONTROL SYSTEM ARCHITECTURE

## Redundant Digital Flight Control System

In most operational modes, the RDFCS is fail-passive, with a dual channel configuration. For automatic landings under Category IIIa conditions (see AC 120-28C), the system can be brought into a dual-dual fail-operational, fail-passive configuration. The classification dual-dual relates primarily to the four computer channels in the system. Each of the two FCCs has two channels which run frame-synchronously, with each channel driving one coil of a dual-coil servo in each axis. Any indication of disagreement between the two channels in an FCC causes the servo connected to that FCC to be disengaged by removing hydraulic pressure. Figure 2.1-1 of this report summarizes the dual-dual configuration.

## Monitoring Configuration and Implementations

Extensive monitoring is employed in the PDFCS for fault detection. Coil current comparators for each servo provide coverage of faults resulting in erroneous commands to the servo coils. They also provide coverage for broken wire faults between the FCC and the servo or failures of the coils themselves. These monitors are made more effective by the insertion of opposing 5 ma bias currents. The bias currents permit circuit integrity to be monitored even when the FCC is not commanding the servo to a new position, such as when the aircraft is flying through very calm air at a stable altitude. It may be noted that this type of monitoring is equally applicable to analog and digital systems.

Response of the autopilot servos to commands from the servo amplifiers is monitored by modulator position signals fed back to the FCC. The feedback signals are averaged and passed through a high-pass filter to get a modulator rate that is compared with cold current. This comparison is used to detect jamming of the modulator piston, runaway conditions, or loss of hydraulic power. This type of monitoring can also be applied to either analog or digital systems.

In the pitch-axis servos, modulator piston position monitoring is implemented in hardware. In the other two axes, it is implemented in software. Together, the coil current monitoring and modulator piston monitoring detect any servo fault which prevents the servo from responding to commands. They also detect any fault in a computer channel which prevents that channel from generating a reasonable command for the servos in each of the three axes. All monitors and feedback sensors are dual to increase reliability.

Each computer channel has an iteration monitor implemented in hardware. This monitor observes the state of a discrete software variable which is changed at the end of each iteration of the foreground software. Since this software executes at a 10 Hertz (Hz) rate, the result is a 10 Hz square wave. Should the processor short-loop or hang up, the 10 Hz wave will not be presented. The iteration monitor will withdraw its input to the engage logic, and the FCC will disengage.

Sensor monitoring is primarily accomplished by comparison and by validity discretes generated by the sensors. There is no one location that sensor monitoring takes place, since all four computer channels incorporate the monitoring function. This process ensures that the circuitry involved in getting the sensor signals to each channel is included in the monitoring.

The accelerometers are tested each time the system is powered up with the airplane on the ground. The ILS receivers are checked using a square wave test. This test checks for failure of the localizer and glideslope beam deviation inputs. During landing, the outputs of both receivers are compared, with reliance on the self-monitoring to identify which receiver is bad if the signals disagree. The comparison monitoring is used to check wire integrity between the receiver and the computer channels. The other dual sensors are comparison monitored in the same way.

Even though each channel monitors sensors individually, any channel can initiate the NO DUAL annunciation, which is the primary indication that the system is not fail-operational. If any channel detects a second failure of a sensor type, it will cause its FCC to disengage, but the other FCC will remain engaged.

Although NO DUAL is the primary warning of loss of one sensor, NO ALIGN will be annunciated if the course signals from the two compass systems do not agree.

Other monitoring within the FCC involves comparison of active operating modes. If the two channels within an FCC disagree on which modes are engaged, and the disagreement lasts for more than 0.1 sec, the FCC will disengage. If the two FCCs disagree, SPLIT will be displayed on the WAIs. This monitoring, together with the sensor data transfers, will detect most faults of the cross-channel data transfer circuitry.

## APPENDIX B - DESCRIPTION OF RDFCS SIMULATOR

The RDFCS simulator is comprised primarily of a PDP 11/60 computer and the RDFCS pallet. The RDFCS pallet includes the FCCs, core memory, MDICU, SSP, DSP, CTA, and Computer Breakout Panels. The functions of these items are described in the remainder of this section. Figures 2.1-2 through 2.1-5 are pictures of these items.

### PDP 11/60 Computer/Airplane Model

The PDP 11/60 computer hosts a discrete-state model of the airplane in which the RDFCS is installed. This airplane is a representative wide-body transport, and the model coefficients are changed according to the flight case being simulated. Each flight case, then, is a point simulation of the airplane in a particular configuration and operating in a specific portion of the flight envelope. The airplane model executes at a 50 Hz rate.

During the subject study (see section 1.2) the flight cases described and discussed in Lockheed-Georgia LG81E0126 (1981) were used in the simulation. As part of this study, a go-around case was added to the library of cases available. The go-around case is characterized as follows:

| | |
|---|---|
| Airplane Weight | 314,500 lb |
| Altitude | 35 ft |
| Angle of Attack | 10.91 ° |
| Indicated Air Speed | 168 kts |
| Flap Deployment | 22 ° |

Transition capability was added to go from approach conditions to landing conditions, and from landing to the new go-around case. The transitions involve changing the model coefficients and establishing new trim values. The transition capability has been installed and checked out successfully.

### Modular Digital Interface Control Unit

The MDICU receives the output of the airplane discrete-state model through a communication link with the PDP 11/60 computer. The MDICU converts the various pieces of information into the form needed by the FCCs. For example, roll angle and pitch angle are converted to three-wire AC signals, properly scaled, while localizer deviation is coded in Aeronautical Radio Incorporated (ARINC) serial digital format. The MDICU is described more fully in the NASA RDFCS System Interface Document.

The MDICU incorporates provisions for the signal for the No. 1 sensor of each type to be ramped up or down. This facility is accessed by means of the HP 2645A terminal physically located in the pallet.

### Computer Breakout Panels

Each sensor signal going from the MDICU to the FCCs can be interrupted at the Computer Breakout Panels by removing the appropriate jumper plug. Every FCC back connector pin is routed through one of these plugs. The lower portion of figure 2.1-3 shows the rows of plugs for connector P1 and the "A" half of connector P2. Each FCC has its own breakout panel.

### CAPS Test Adapters

Figure 2.1-3 also shows the CTA for one of the FCCs. The upper half of the CTA includes, on the right-hand side, four address and four data windows. An address can be loaded in each address window. The corresponding data window can be used to display the data on the FCC A-side processor bus data lines every time the address appears on the address lines. The CTA also has other capabilities, such as providing a history of the last 16 bus transfers and changing the contents of a specific memory location within the FCC, but during the subject study only the address monitoring was used. Discrete variables representing sensor voter status were monitored visually via the data windows. Continuous variables, such as inputs to the servo amplifiers, were monitored by using the analog output posts below the appropriate data window to drive a strip-chart recorder.

The lower half of the CTA performs the same functions as the upper half, but for the B side of the FCC.

### Servo Simulator Panel

The servo amplifier outputs from the FCCs are routed to the SSP. The SSP simulates the dynamics of the autopilot and power servos, and generates the required feedback signals such as modulator piston position. The SSP has circuits which can simulate a hardover or slowover command to a servo coil. It can also simulate a hardover or slowover of a modulator piston, including the modulator piston position feedback signal and the command to the power servo. All of these apply to the No. 1 servo of each type.

### Discrete Switch Panel

The DSP is located just below the SSP. This panel provides a centralized location for switches such as hydraulic pressure switches and autopilot disconnect switches. The panel also includes switches that can be used to insert sensor validity faults. These faults can also be inserted by pulling the appropriate jumper plug on the FCC Breakout Panel.

### Core Memory

The pallet also contains core memory for the FCCs. This is used for both data and program memory to provide flexibility and convenience in using the pallet to simulate other airplanes or DFCS architectures. As used in an airplane, the FCCs have the flight software stored in PROM and use Random Access Memory (RAM) chips for data memory.

### Glare-Shield Panel

The pallet also has a glare-shield panel, which is the control panel for the system as installed in an airplane. It includes the engage (bat handle) switches, mode select switches, altitude select knob, and other controls. The pallet also has a single Automatic Direction Indicator (ADI), Horizontal Situation Indicator (HSI), radio altitude display, Mode Indicator, and WAI.

# APPENDIX C - FAILURE MODES AND EFFECTS ANALYSIS RESULTS

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Instruction Mapper Prom CU1 | Produce direct input bits A0-A3 for control store memory microprogram start address | A0-A9 | Open | Address bit low, wrong address read. Wrong output passed to control store proms as starting address bits A0-A3. Massive processor failure. |
| | | | Low | Address bit sticks, wrong address read. Wrong output passed to control store proms as starting address. Massive processor failure. |
| | | | High | Same as above |
| | | CS1, CS2 | Open | Output pins remain in high-impedence state. Input pins to microprogram sequencer CU16 low. Wrong starting address bits A0-A3 to control store proms. Massive processor failure. |
| | | | Gnd | Don't care. |
| | | | High | Same as open. |
| | | 01-04 | Open | Prom output bit not fed to microprogram sequencer input bit. Input bit low, resulting in wrong microprogram starting address. Massive processor failure. |
| | | | Low | Corresponding bit (A0-A3) of microprogram start or jump address is always low. Massive processor failure. |
| | | | High | Corresponding bit (A0-A3) of microprogram start or jump address is always high. Massive processor failure. |
| Instruction Mapper Prom CU7 | Produce direct input bits A4-A7 for control store memory microprogram start address. | | | The fault of any pin of CU7 has the same effect as the same fault occurring in CU1, except that the affected address bits are A4-A7. |

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Instruction Mapper Prom CU13 | Produce direct input bits A8-A9 for control store memory microprogram start address; produce push/pop signals to stack vector register DU4. | A0-A9 | Open | Address bit low, wrong address read. Wrong output passed to control store proms as starting address bits A8-A9. Wrong output may also include wrong push or pop signal to stack vector. |
| | | | Low | Address bit stuck low, wrong address read. Bits A8-A9 of microprogram start address wrong. Push or pop signal to stack vector register DU4 may be wrong. Massive processor failure. |
| | | | High | Address bit stuck high, wrong address read. Bits A8-A9 of microprograms start address wrong. Push or pop signal to stack vector register DU4 may be wrong. Massive processor failure. |
| | | CS1, SS2 | Open | Control register cannot pull down enable, so that output pins are at high impedance. Start address bits A8-A9 always low. Massive processor failure. |
| | | | Low | Chip CU13 can pull down data input to microprogram sequencer when control register is trying to set it high as part of a jump address. |
| | | | High | Same as open. |
| | | 01-02 | Open | Start address bit A8, A9 to control store always low. Massive processor failure. |
| | | | Low | Same as open. |
| | | | High | Start address bit A8, A9 high; address bad when bit should be low. Massive processor failure. |

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| CU13 con't. |  | 03-04 |  |  |
|  |  |  | Low | POP commanded (pin 03 faulted) or PUSH commanded (pin 04 faulted) on each clock pulse, so that both commands will go to stack vector register when only non-faulted should be. Stack vector register will do nothing. Massive processor failure. |
|  |  |  | High, Open | Fault in pin 03 causes stack vector register to broadside load instead of left shift when mapper prom tries to pop stack. Fault in pin 04 causes broadside load instead of right shift when mapper prom tries to push stack. Stack pointer not pointing to top of stack. Massive processor failure. |
| Microprogram Sequencer CU14 | Generate sequence of microcode Code addresses for control store proms using starting address from mapper or control register. U14 generates microcode address bits A8,A9 | DO, DI | Open | Address bit A8, A9 to control store proms always low when starting microcode sequence or on microcode jump. Massive processor failure. |
|  |  |  | Gnd | Same as above |
|  |  |  | High | Same as above, except that affected bit is always high. |
|  |  | CN | Open | Carry-in from microprogram sequencer CU15 is alway low. Wrong address will be sent to control store when address increment causes overflow in CU15. Effect depends on allocation of control store store addresses to microcode sequences. |
|  |  |  | Gnd | Same as above |

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| CU14 con't. | | | High | In incrementing address register, bit A. will be toggled on each clock pulse. Wrong micro-code address will be generated during most microcode sequences. Massive processor failure. |
| | | OE | Open | Address bits A8, A9 always low. |
| | | | Gnd | No effect during operation. Maintenance trouble-shooting affected. |
| | | RE | Open | Initial microsequence address from mapper prom cannot be loaded. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | No effect. |
| | | SO | Open | Sequencer will not jump to proper address when SO should be high. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Sequencer will execute erroneous jump when SO should be low. Massive processor failure. |
| | | SI | | Same effect as pin SO faulted. |
| | | FE | Open<br>* | Microprogram counter will always be pushed onto stack or stack will be popped, depending on PUP. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Microprogram counter cannot be pushed on stack and stack cannot be popped. Massive processor failure. |

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Microprogram<br>Sequencer<br>CU14 con't. | | PUP | Open | Stack will be popped when microprogram counter should be pushed on stack. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Microprogram counter will be pushed onto stack when stack should be popped. Massive processor failure. |
| | | CP | Any | Chip disabled. CP is clock pulse input, and all state changes occur on low-to-high transition of CP. Massive processor failure. |
| | | ZERO | Open | Address bits A8, A9 to control store proms always low. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Address bits A8, A9 not forced low when commanded by control register CU21. Effect depends on implementation of microcode. |
| | | Y0, Y1 | Open | Corresponding address bit to control store is always low. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Corresponding address bit to control store is always high. Massive processor failure. |
| | | Y2<br>CN+4,<br>D2,D3 | Any | No effect. Pins not connected. |
| | | VCC | Open | Chip dead. Massive processor failure. |
| | | Gnd | Open | Chip dead. Massive processor failure. |

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Microprogram Sequencer CU15 | Generate address bits A4-A7 to control store proms. Effects of most pin faults are the same as for CU14, except 'he affected address bits are A4-A7. Only pins with different fault are discussed. | D2,D3 | Open | Corresponding address bit A6 or A7 is always when address is from mapper prom or microcoded jump address. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Corresponding address bit A6 or A7 is always high when address is from mapper prom or microcoded jump address. Massive processor failure. |
| | | CN | Open | Carry-in from microprogram sequencer CU14 is always low. Wrong address will be sent to control store when address increment causes overflow in CU14. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Carry-in from microprogram sequencer CU14 is always high. Microcode address incremented on bit A4 each clock cycle. Massive processor failure. |
| | | CN+4 | Open | Same as CN open on CU14. |
| | | | Gnd | Same as above. |
| | | | High | Same as CN high on CU14. |
| | | Y2,Y3 | Open | Corresponding bit A6 or A7 always low in address to control store. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Corresponding bit A6 or A7 always high in address to control store. Massive processor failure. |

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Microprogram Sequencer CU16 | Generate address bits A0-A3 to control store proms. Effects of most pin faults are the same as for CU15, except that affected address bits are A0-A3. Only pins with different effects are discussed. | CN | Open | Microprogram address is not incremented during execution of microcode sequence. Massive processor failure. |
| | | | Gnd | Same as above. |
| Micro-processor BU17 | Processes the four low-order bits of the 16-bit CAPS word in response to instructions from control registers. | A0-A3 | Open | Wrong A pointer address when failed bit should be high. Massive processor failure. |
| | | | Gnd. | Same as above. |
| | | | High | Wrong A pointer address when failed bit should be low. Massive processor failure. |
| | | B0-B3 | Open | Wrong B pointer address when failed bit should be high. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Wrong B pointer address when failed bit should be low. Massive processor failure. |
| | | I0-I2 | Open | Wrong data source selected when failed bit should be high. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Wrong data source selected when failed bit should be low. Massive processor failure. |

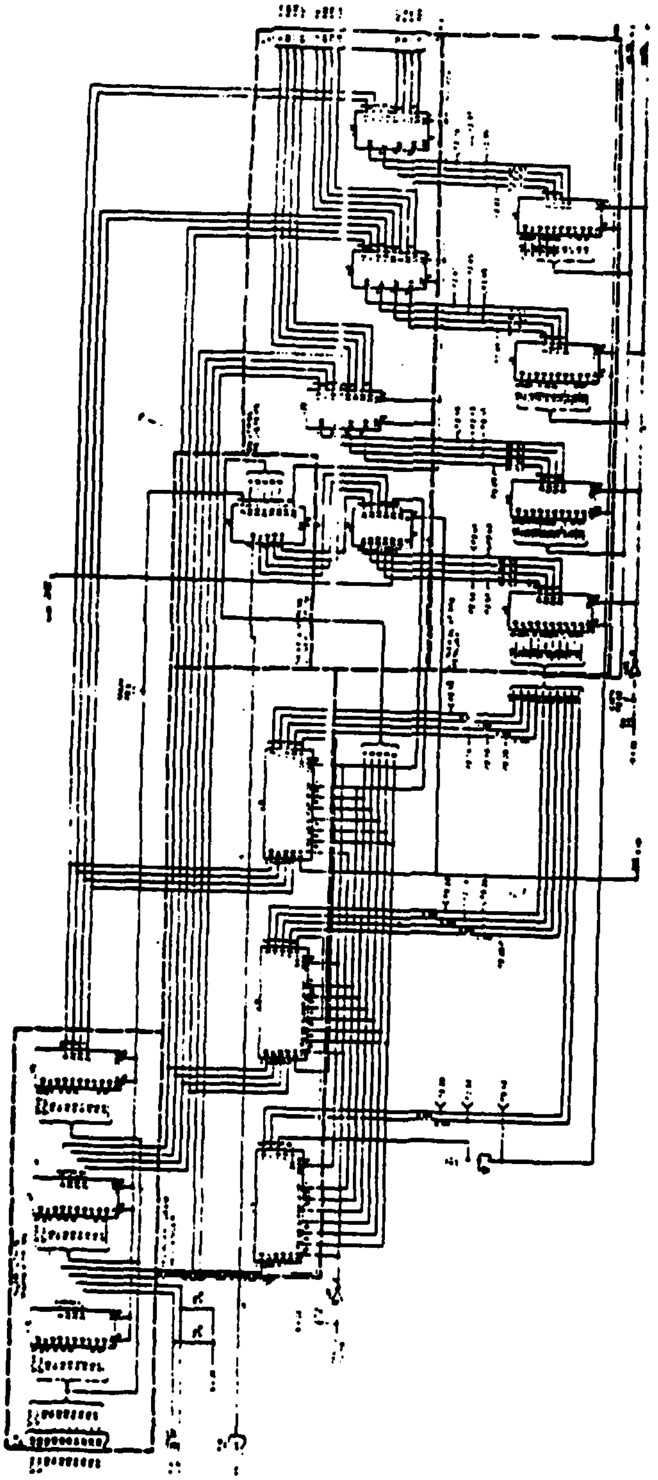
| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Micropro-cessor DU17 | | I3-I5 | Open | Wrong operation performed when failed bit should be high. Massive processor failure. |
| | | | Gnd | Same as above. |
| | | | High | Wrong operation performed when failed bit should be low. Massive processor failure. |
| | | I6-I8 | Open | Wrong destination code when failed bit should be high. In most cases, the immediate effect will be internal to the chip involving load or shift of data in registers. Massive processor failure. |
| | | | Gnd. | Same as above. |
| | | | High | Wrong destination code when failed bit should be low. Massive processor failure. |
| | | CP | Any | Chip dead. Massive processor failure. |
| | | DO-D3 | Open | Input to processor is wrong when failed bit should be high. Major effect caused by incorrect bit in packed Boolean data. Massive processor failure. |
| | | | Gnd. | Same as above. |
| | | C | Open | Carry-in always low. Program counter not incremented on instruction fetch. Massive processor failure. |
| | | | Gnd. | Same as above. |
| | | | High | Carry-in always high. Foreground loop of flight software cannot execute paths 2 and 4; iteration monitor test bit not toggled; iteration monitor trips. FCC disconnects. |

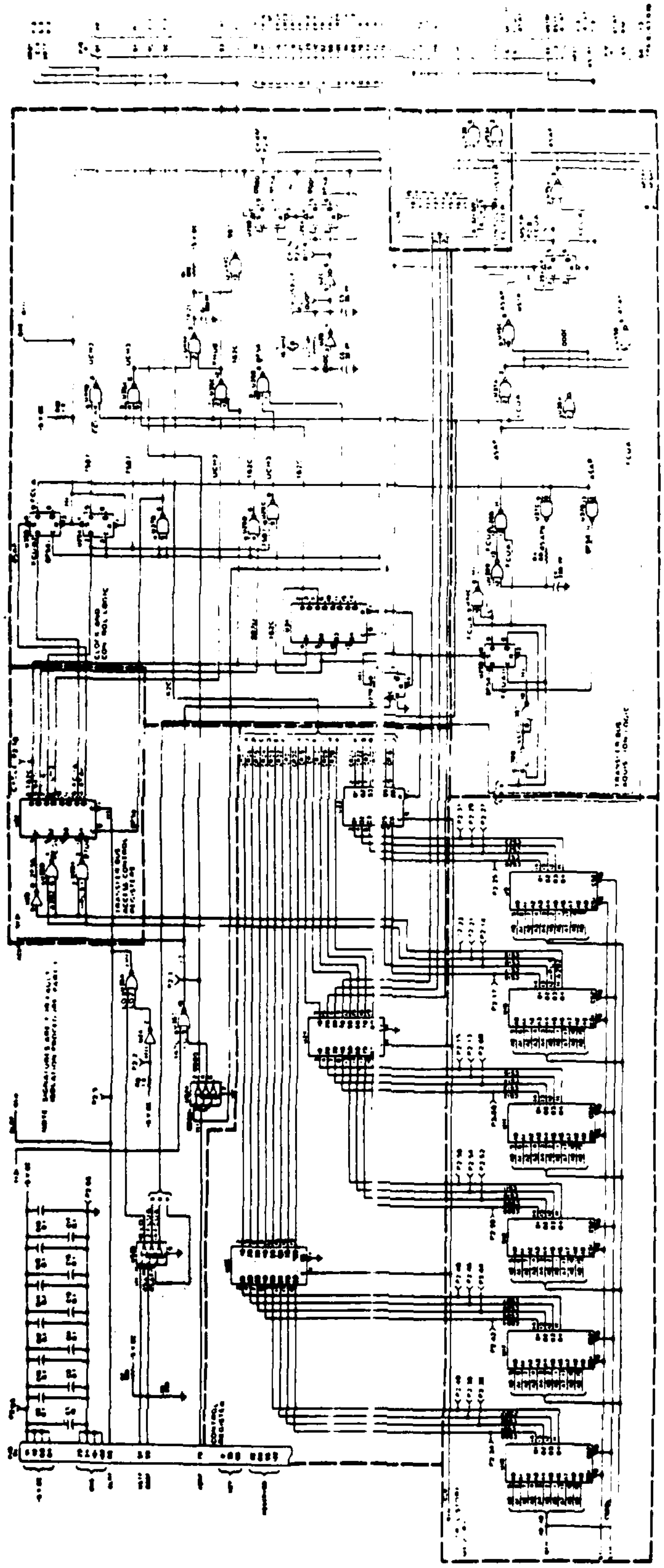
| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Micropro-<br>cessor DU17<br>con't. |  | Y0-Y3 | Open | Wrong address gated on CAPS address lines. Massive processor failure. |
|  |  | P | Open | Carry propagate always sent to carry look-ahead logic. Massive processor failure. |
|  |  |  | Gnd | Same as above. |
|  |  |  | High | Carry propagate never sent to carry look-ahead logic. Double-precision integrators drift. |
|  |  | G | Open | Carry generate always sent to carry look-ahead logic. Massive processor failure. |
|  |  |  | Gnd | Same as above. |
|  |  |  | High | Carry generate signal never sent to carry look-ahead logic. |
|  |  | F=0 | Open | DU17 cannot pull down F=0 line to status register, yielding false results for some logic tests. Massive processor failure. |
|  |  |  | Gnd | DU17 always pulls down F=0 line to status register yielding false results for some logic tests. Massive processor failure. |
|  |  |  | High | Same as open. |
|  |  | Vcc | Open | Chip dead. Massive processor failure. |
|  |  | OE | Open | Chip dead. Massive processor failure. |
|  |  | Gnd | Open | Chip dead. Massive processor failure. |
|  |  | R3 | Open | Bit left-shifted into DU14 or right shifted into DU17 always low. Multiplication results erroneous. FCC disconnect. |
|  |  |  | Gnd | Same as above. |

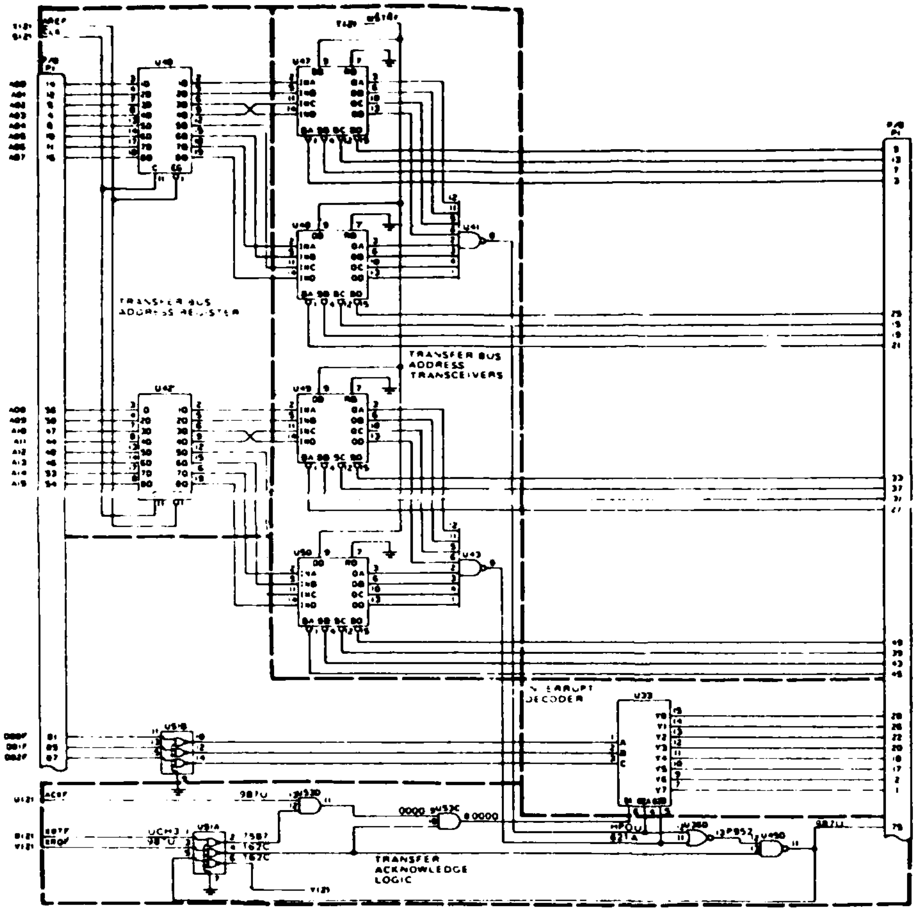
| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Micropro-cessor DU17 cont't. | | | High | Bit left-shifted into DU14 or right-shifted into DU17 always high. Multiplication results erroneous. FCC disconnect. |
| | | Ro | Open | Bit right-shifted to shift/rotate multiplexer or input from shift/rotate multiplexer always low. Multiplication results erroneous. FCC disconnects. |
| | | | Gnd | Same as above. |
| | | R0 | High | Bit right-shifted to shift/rotate multiplexer or input from shift/rotate multiplexer always high. |
| | | Q3 | Open | Bit right-shifted into DU17 or left-shifted to DU14 always low. Multiplication results erroneous. FCC disconnects. |
| | | | Gnd | Same as above. |
| | | | High | Bit right-shifted into DU17 or left-shifted to DU14 always high. Multiplication results erroneous. FCC disconnects. |
| | | Q0 | Open | Bit right-shifted to shift/rotate multiplexer or left shifted from shift/rotate multiplexer always low. Multiplication results erroneous. FCC disconnects. |
| | | | Gnd | Bit right-shifted to shift/rotate multiplexer. or left-shifted from shift/rotate multiplexer always high. Multiplication results erroneous. FCC disconnects. |
| | | F3 | Any | No effect. Pin not connected. |
| | | CN+4 | Any | No effect. Pin not connected. |
| | | OVR | Any | No effect. Pin not connected. |

| Circuit | Function | Pin | Fault | Effect |
|---|---|---|---|---|
| Micro-processor DU14 | Microprocessor DU14 handles bits 4-7 of the 16-bit APS word in response to instructions from the control registers. Effect of fault as if fault had occurred on DU17, except that different bit positions in the CAPS word are affected. | | | |
| Micro-processor DU18 | Microprocessor DU18 handles bits 8-11 of the 16-bit CAPS word in response to instructions from the control registers. Effect of pin faults is the same as if the fault had occurred on DU17, except that different bit positions in the CAPS word are affected. | | | |
| Micro-processor DU15 | Microprocessor DU15 handles bits 12 - 15 of the 16-bit CAPS word in response to instructions from the control registers. Effect of pin faults is the same as if the fault had occurred in DU14, except that different bits are affected. Some differences result from the use of bit 15 as the sign bit in numerical computation. | | | |

# APPENDIX D - PROCESSOR SCHEMATIC DIAGRAMS

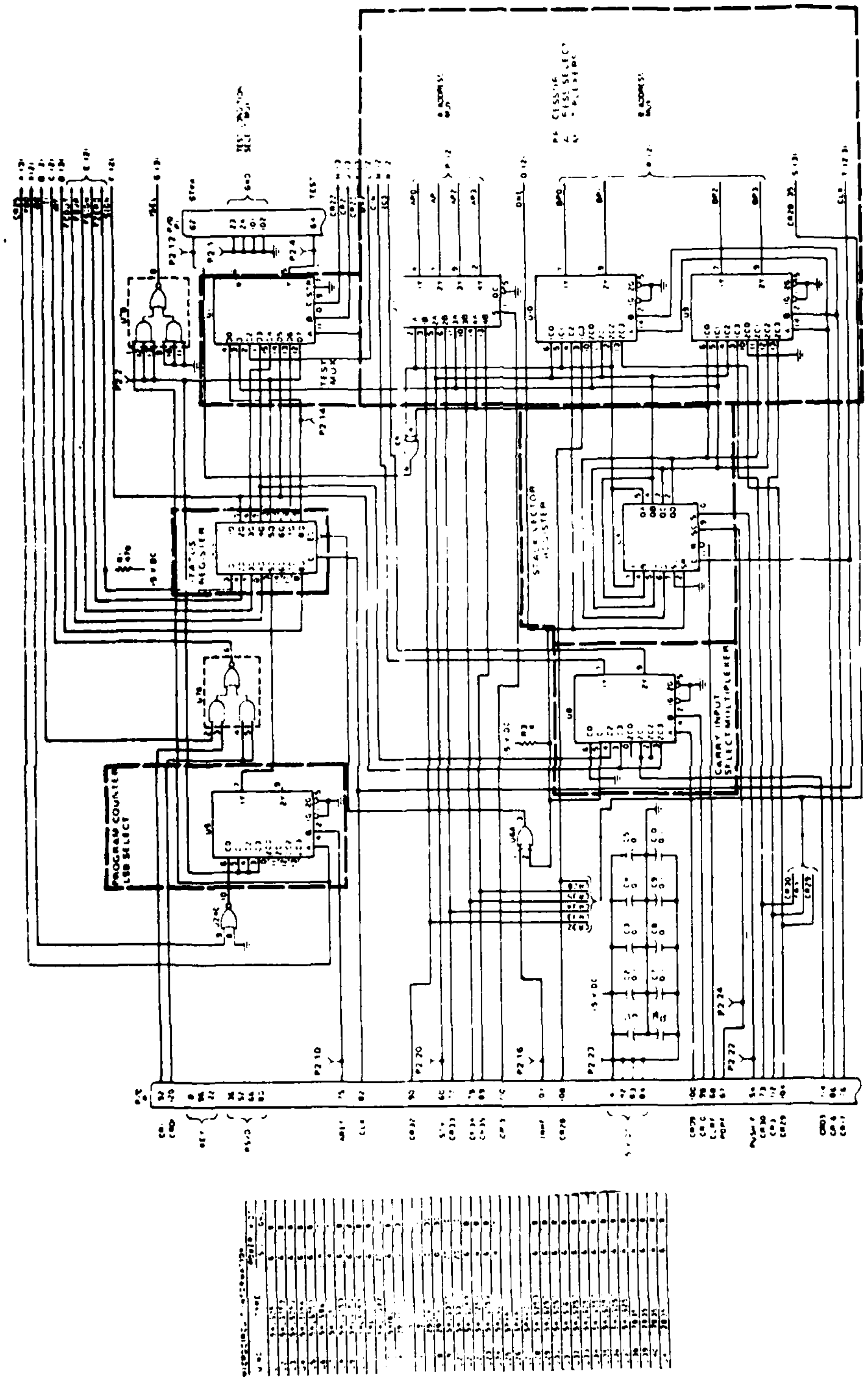




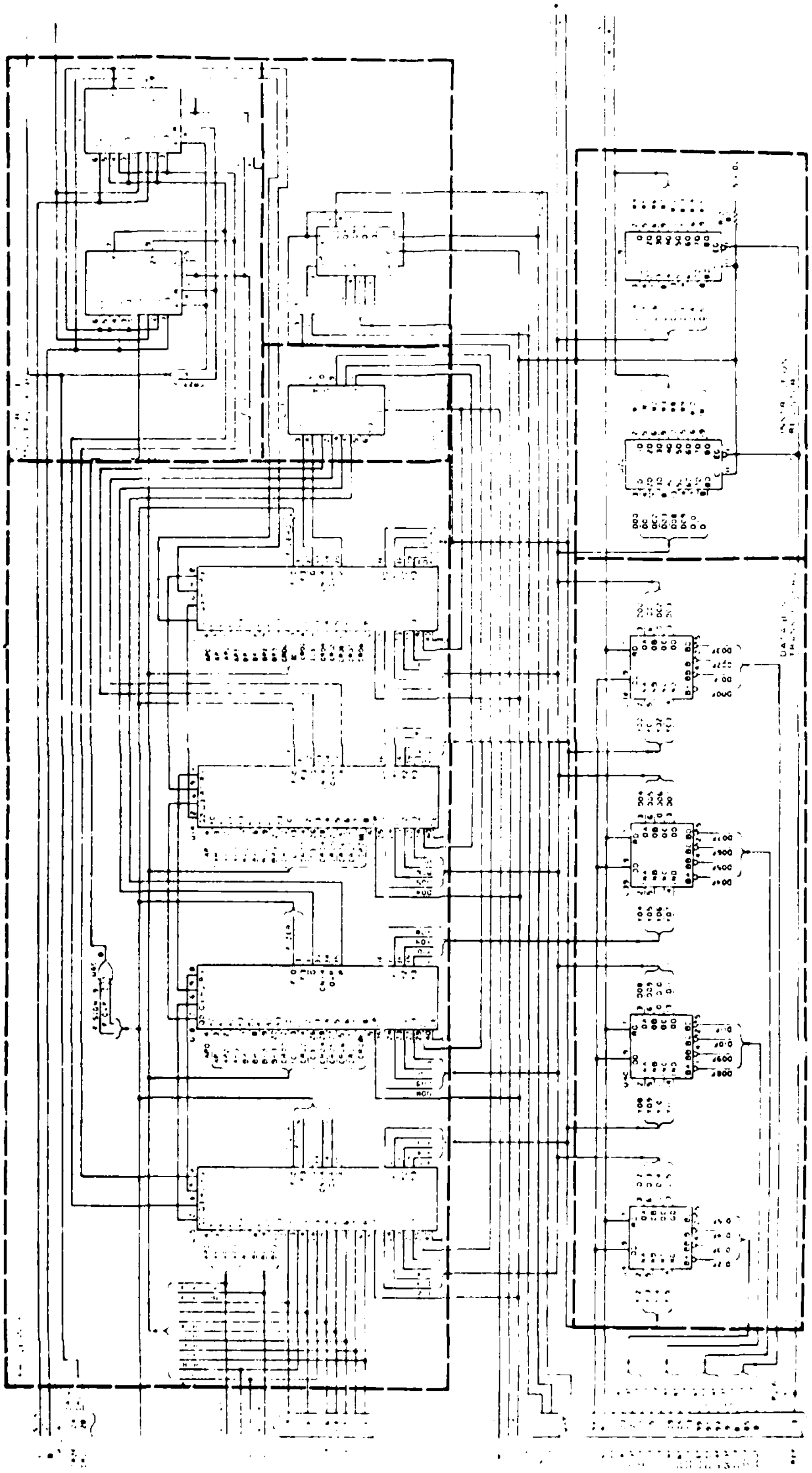


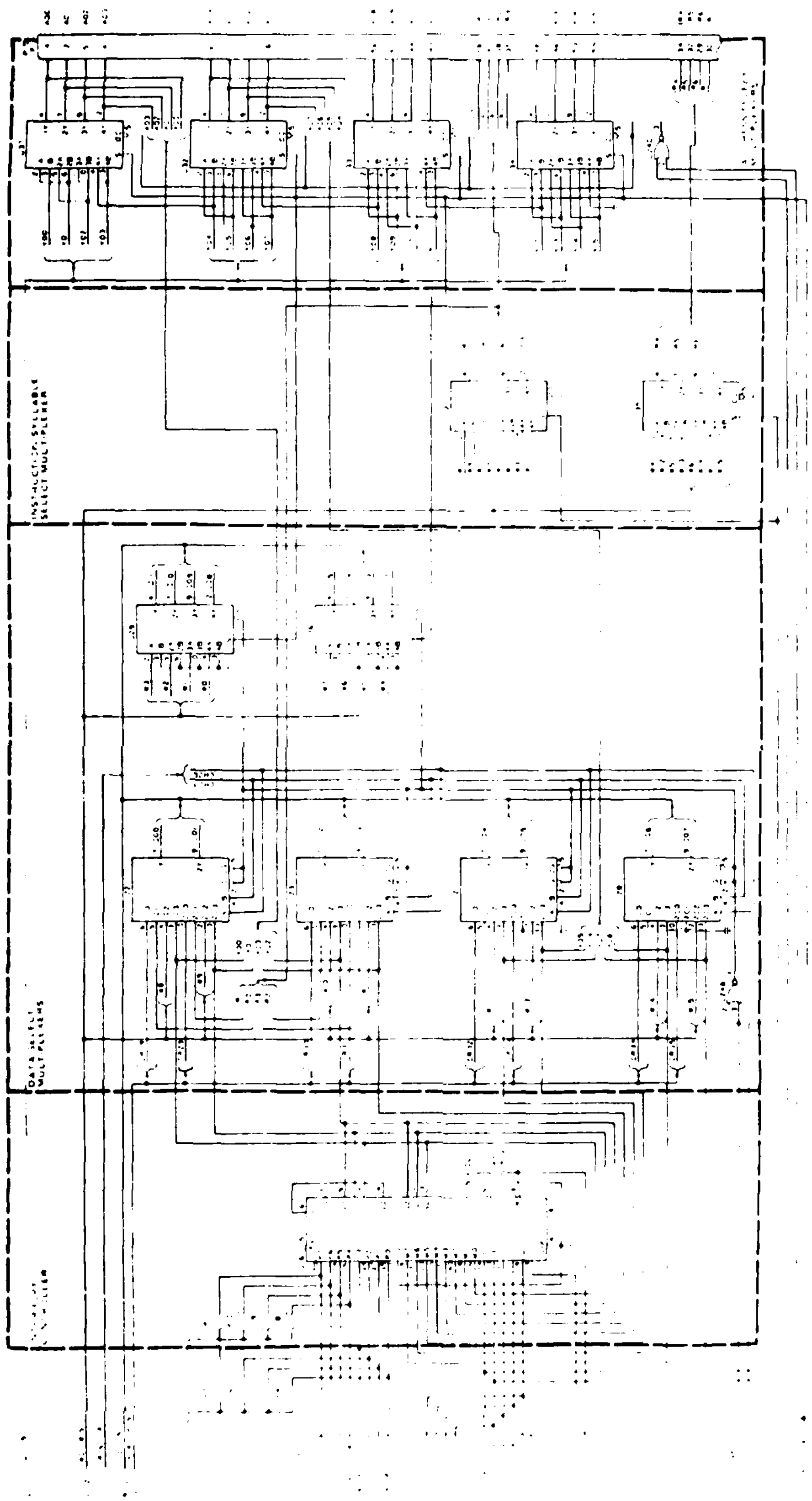
| U NO. | TYPE | POWER PINS | |
|---|---|---|---|
| | | +5 | GND |
| U1 | HM7643 | 18 | 9 |
| U2 | 5404 | 14 | 7 |
| U3 | HM7643 | 18 | 9 |
| U4 | HM7643 | 18 | 9 |
| U5 | HM7643 | 18 | 9 |
| U6 | HM7643 | 18 | 9 |
| U7 | HM7643 | 18 | 9 |
| U8 | HM7643 | 16 | 8 |
| U9 | HM7643 | 18 | 9 |
| U10 | HM7643 | 18 | 9 |
| U11 | HM7643 | 18 | 9 |
| U12 | HM7643 | 18 | 9 |
| U13 | HM7643 | 18 | 9 |
| U14 | 2901 | 2 | 0 |
| U15 | 2901 | 2 | 0 |
| U16 | 2901 | 2 | 0 |
| U17 | HM7643 | 18 | 9 |
| U18 | HM7643 | 18 | 9 |
| U19 | NOT USED | | |
| U20 | 5474 | 14 | 7 |
| U21 | 54LS174 | 16 | 8 |
| U22 | 54LS175 | 16 | 8 |
| U23 | 54LS174 | 16 | 8 |
| U24 | 54LS377 | 20 | 10 |
| U25 | 54LS377 | 20 | 10 |
| U26 | NOT USED | | |
| U27 | 54LS112 | 16 | 8 |
| U28 | 54LS00 | 14 | 7 |
| U29 | 54LS74 | 14 | 7 |
| U30 | 29LS18 | 16 | 8 |
| [illegible] | [illegible] | [illegible] | [illegible] |
| U32 | 29LS18 | 16 | 8 |
| U33 | 54LS138 | 16 | 8 |
| U34 | 54LS175 | 16 | 8 |
| U35 | 5402 | 14 | 7 |
| U36 | 54LS02 | 14 | 7 |
| U37 | 5437 | 14 | 7 |
| U38 | 54LS32 | 14 | 7 |
| U39 | 5474 | 14 | 7 |
| U40 | 54LS377 | 20 | 10 |
| U41 | 54LS32 | 14 | 7 |
| U42 | 54LS377 | 20 | 10 |
| U43 | 54LS30 | 14 | 7 |
| U44 | 5430 | 14 | 7 |
| U45 | 5438 | 14 | 7 |
| U46 | 54LS138 | 16 | 8 |
| U47 | 7835 | 16 | 8 |
| U48 | 7835 | 16 | 8 |
| U49 | 7835 | 16 | 8 |
| U50 | 7835 | 16 | 8 |
| U51 | 7837 | 16 | 8 |
| U52 | 7837 | 16 | 8 |
| U53 | 54LS00 | 14 | 7 |
| | | | |

NOTE SIGNATURES ARE FOR FAULT ISOLATION PROCED [illegible] PART [illegible]



PROGRAM COUNTER LSB SELECT
STATUS REGISTER
STACK VECTOR REGISTER
CARRY INPUT SELECT MULTIPLEXER
TEST MUX
+5 VDC
P2 10
P2 14
P2 16
P2 20
P2 22
P2 23
P2 24




INSTRUCTION SYLLABLE
SELECT MULTIPLEXER
DATA SELECT
MULTIPLEXERS

# APPENDIX E - RESULTS OF FAULT INSERTION

## COMPONENT LEVEL FAULTS

|  | ADDRESS | FB03 | FB01 | 3635 | 3318 | FB03 | FB01 | 32E6 | 331A |  |
|---|---|---|---|---|---|---|---|---|---|---|
| CASE | VARIABLE | VG #1 | $\dot{\theta}$ #1 | AP. ONE FAIL | EXEC FAIL θ | VG #3 | $\dot{\theta}$ #3 | EXEC FAIL θ | EXEC FAIL $\dot{\theta}$ |  |
|  | Strip Chart | 1 | 2 |  |  | 3 |  |  |  |  |
| 1A | Vert. Gyro #1 X-Leg open Inbound |  |  | 0000<br>0001 | 0000<br>0003 |  |  | 0000<br>0003 | 0000<br>0003 | Pin PIA-31, X-Leg V.G. #1 Open On Pin removal; ATS Disconnect warning - NO DUAL, NO ALIGN at 1500 ft. |
| 1B | Vert. Gyro #1 Y Leg open Inbound |  |  | 0000<br>0000<br>0000 | 0000<br>0003<br>0000 |  |  | 0000<br>0003<br>0000 | 0000<br>0000<br>0000 | On pin removal ATS disconnect; prior to A/L track AP.ONEFAIL was cleared. |
| 2A | Vert. Gyro #1 hard shift to fixed value Inbound |  |  | 0000<br>0001 | 0000<br>0003 |  |  | 0000<br>0003 | 0000<br>0000 | First fault was not of sufficient magnitude to fault sys., fault level was increased resulting in the CTA values shown, NO DUAL was annunciated upon engagement of A/L TRK. |
| 2B | Same as 2A but in AL. Arm |  |  | 0000<br>0001<br>0000 | 0000<br>0003<br>0003 |  |  | 0000<br>0003<br>0003 | 0000<br>0000<br>0000 | ATS Disc. WRN. on insertion NO DUAL did not light. AP.ONEFAIL reset. |
| 2C | Same as 2A but in AL. TRK above 150 ft |  |  | 0000<br>0000 | 0000<br>0003 |  |  | 0000<br>0003 | 0000<br>0000 | ATS. dropped out on insertion, no ATS warning; NO DUAL did not annunciate |
| 2D | Same as 2A but in AL. TRK below 150 ft. |  |  | 0000<br>0000 | 0000<br>0003 |  |  | 0000<br>0003 | 0000<br>0000 | NO DUAL did not annunciate |
| 2E | Vert. Gyro #1 Validity false Inbound |  |  | 0000<br>0001 | 0000<br>0000 |  |  | 0000<br>0000 | 0000<br>0000 | NO DUAL did not annunciate |

# COMPONENT LEVEL FAULTS

| CASE | ADDRESS<br>VARIABLE | FB03<br>VG #1 | FB01<br>$\dot{\theta}$ #1 | 3635<br>AP. ONE<br>FAIL | 3318<br>EXEC<br>FAIL θ | FB03<br>VG #3 | FB01<br>$\dot{\theta}$ #3 | 32E6<br>EXEC<br>FAIL θ | 331A<br>EXEC<br>FAIL $\dot{\theta}$ | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Strip Chat | | | | | | | | | |
| 3A | Vert. Gyro #1 | | | 0000 | 0000 | | | 0000 | 0000 | Disconnect of ATS on Insertion; |
| | Open X-Leg In | | | 1 | 0000 | | | 0000 | 0000 | No dual annunciated. |
| | AL.ARM | | | | | | | | | |
| 3B | Vert. Gyro #1 | | | 0000 | 0000 | | | 0000 | 0000 | ATS Disc. on Insertion. |
| | Open Y-Leg In | | | 1 | 3 | | | 3 | 3 | No dual annunciated. |
| | AL.ARM | | | 0 | 3 | | | 3 | 0 | Exec. Fail Resets |
| 4A | Vert. Gyro #1 | | | 0000 | 0000 | | | 0000 | 0000 | No dual annunciation, ATS |
| | Open X Leg In | | | 1 | 3 | | | 3 | 3 | Disc. Announ. ATS Disc. |
| | AL.TRK above | | | | | | | | | |
| | 150 Ft. | | | | | | | | | |
| 4B | Vert. Gyro #1 | | | 0000 | 0000 | | | 0000 | 0000 | No dual & ATS Disc.annunciated, |
| | Open Y Leg | | | 1 | 3 | | | 3 | 3 | ATS Disc. |
| | AL.TRK above | | | | | | | | | |
| | 150 Ft. | | | | | | | | | |
| 5A | Same as 4A but | | | 0000 | 0000 | | | 0000 | 0000 | ATS Disconn. without annunciation. |
| | below 150 Ft. | | | 1 | 3 | | | 3 | 3 | No dual not Indicated. |
| 5B | Same as 4B but | | | 0000 | 0000 | | | 0000 | 0000 | No dual did not Indicate, ATS |
| | below 150 Ft. | | | 0 | 3 | | | 3 | 0 | Disc. & Ind. |

## COMPONENT LEVEL FAULTS

| | ADDRESS | FB03 | FB01 | 3635<br>AP. ONE | 3318<br>EXEC | FB03 | FB01 | 32E6<br>EXEC | 331A<br>EXEC | |
|---|---|---|---|---|---|---|---|---|---|---|
| CASE | VARIABLE | VG #1 | $\dot{\theta}$ #1 | FAIL | FAIL θ | VG #3 | $\dot{\theta}$ #3 | FAIL θ | FAIL $\dot{\theta}$ | |
| | Strip Chnl | | | | | | | | | |
| 6 | Vert. Gyro #1 | | | 0000 | 0000 | | | 0000 | 0000 | No dual flashed but did not |
| | Ramp Up | | | 1 | 3 | | | 3 | 0 | latch. |
| | Inbound | | | 0 | 3 | | | 3 | 0 | 3635 reset when no dual flashed. |
| 7 | Vert. Gyro #1 | | | 0000 | 0000 | | | 0000 | 0000 | No dual indicated. |
| | Ramp Down | | | 1 | 3 | | | 3 | 0 | |
| | Inbound | | | | | | | | | |
| 8A | Vert. Gyro #3 | | | 0000 | 0000 | | | 0000 | 0000 | |
| | Open X-Leg | | | 1 | 2 | | | 2 | 0 | |
| | Inbound | | | 0 | 2 | | | 2 | 0 | At 1500 Ft. No dual lit |
| 8B | Vert. Gyro #3 | | | 0000 | 0000 | | | 0000 | 0000 | No dual flashed, Reset 3635, |
| | Open Y Leg | | | 1 | 2 | | | 2 | 0 | ATS Disc. Warning but ATS stayed. |
| | Inbound | | | 0 | 2 | | | 2 | 0 | |

## COMPONENT LEVEL FAULTS

| CASE | ADDRESS VARIABLE | FBIF<br>N.A.#1 | 3380<br>N.A.EXEC.<br>FAIL | 3635<br>ARONE<br>FAIL | FBIF<br>N.A.#3 | 334E<br>EXEC.<br>FAIL | |
|---|---|---|---|---|---|---|---|
| | Strip Chnl | 1 | | | 3 | | |
| 9A | Norm. Accel. #1<br>Open signal<br>Inbound | | 0000<br>0 | 0000<br>0 | | 0000<br>0 | ATS held in; ATS Disc. warning at A/L TRK. |
| | | | 0000<br>3 | 0000<br>1 | | 0000<br>3 | Case 9A repeated with turbulence; Fault detected & NO DUAL |
| 9B | Norm. Accel. #1<br>Open Gnd.<br>Inbound | | 0000 | 0000 | | 0000 | Case 9B involved signal gnd. Pulling pin has no effect. |

## COMPONENT LEVEL FAULTS

### FCC # 1 CTA WINDOW

| CASE | ADDRESS VARIABLE<br>STRIP CHNL | A1<br>FB07<br>ROLL<br>RATE 1 | A2<br>FB05<br>ROLL<br>RATE 1 | A3<br>3635<br>A.P.ONE<br>FAIL | A4<br>33E8<br>EXEC.<br>FAIL ROLL | B1<br>FB07<br>ROLL<br>RATE 3 | B2<br>FB05<br>ROLL<br>RATE 3 | B3<br>3386<br>EXEC.<br>FAIL ROLL | B4<br>33EA<br>EXEC.<br>FAIL ROLL | |
|---|---|---|---|---|---|---|---|---|---|---|
| 10A | Roll Gyro #1 Open X-Leg in AL.ARM | | | 0000<br>1 | 0000<br>3 | | | 0000<br>3 | 0000<br>3 | No dual at A/L TRK |
| 10B | Roll Gyro #1 Open Y Leg in AL.ARM | | | 0000<br>1 | 0000<br>• 3 | | | 0000<br>3 | 0000<br>0 | No dual at A/L TRK |
| 11A | Roll Gyro #1 Ramp Up Inbound | | | 0000 | 0000 | | | 0000 | 0000 | No dual at A/L TRK |
| 11B | Same as 11A but in AL.ARM | | | 0000<br>1 | 0000<br>3 | | | 0000<br>3 | 0000<br>0 | No dual at 1100 FT. (When Comparators Tripped). |
| 11C | Same as 11A | | | 0000<br>1 | 0000<br>3 | | | 0000<br>3 | 0000<br>0 | No dual at 1100 FT. (When Comparators Tripped). |
| 11D | Same as 11A but in AL.TRK below 150 Ft. | | | 0000<br>1 | 0000<br>3 | | | 0000<br>3 | 0000<br>0 | Landing Completed Without No Dual Indication. |

## COMPONENT LEVEL FAULTS

FCC # 1 CTA WINDOW

| CASE | ADDRESS VARIABLE<br><br>STRIP CHNL | A1<br>FBIB<br>LOC.DEV.<br># 1 | A2<br>339A<br>EXEC.FAIL<br>LOC.DEV. | A3 | A4<br>33E8 | B1<br>FBIB<br>LOC.DEV.<br># 1 | B2<br>3368 | B3 | B4<br>33EA | |
|---|---|---|---|---|---|---|---|---|---|---|
| 12A | No Localizer Output In Inbound | | 0000<br>6003<br>4003 | | 0000<br>0 | | 0000<br>6003<br>4003 | | 0000<br>0 | No dual at AL.TRK |
| 12B | Same as 12A but in AL.ARM | | 0000<br>4003 | | 0000<br>0000 | | 0000<br>4003 | | 0000<br>0000 | No dual indicated when fault detected (at 1000 Ft.) |
| 12C | Same as 12A but in AL.TRK above 150 Ft. | | 0000<br>4003 | | 0000<br>0000 | | 0000<br>4003 | | 0000<br>0000 | No dual indicated when fault detected (at 1000 Ft.) |
| 12D | Same as 12A but in AL.TRK below 150 Ft. | | 0000<br>6003 | | 0000<br>0000 | | 0000<br>6003 | | 0000<br>0000 | Fault detected; Land completed; No dual did not illuminate. |
| 14A | Localizer No. 1, Validity 1 in AL. ARM | | 0000<br>4013 | | 0000 | | 0000<br>4013 | | 0000 | No dual at AL.TRK |
| 14B | Localizer No. 1, Validity 2 in AL. ARM | | 0000<br>4023 | | 0000 | | 0000<br>4023 | | 0000 | No dual at AL.TRK |
| 16 | Lateral Accel. No. 1 Ramp Up in AL. ARM | FBID | 33B4 | 33B4<br>EXEC.FAIL<br><br>0000<br>400A | 3635<br>AP. ONE<br>FAIL<br>0000 | FBID | | 33B2<br>EXEC.FAIL<br><br>0000<br>400A | 3635<br>AP.ONE<br>FAIL<br>0000 | No dual at 1100 Ft. when comparator tripped. |

## COMPONENT LEVEL FAULTS

## FCC #1 CTA WINDOW

| CASE | ADDRESS VARIABLE | A1 | A2 | A3 | A4 | B1 | B2 | B3 | B4 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 3364 | 3365 | | | 3364 | 3365 | |
| | | | | AP.TWO | AP.ONE | | | AP.TWO | AP.ONE | |
| | STRIP CHNL. | | | FAIL | FAIL | | | FAIL | FAIL | |
| 17A | Pitch Servo Coil Discrete Fault Inbound | | | 0000 | 0000 | | | 0000 | 0000 | Instant disengage; No dual at A/L TRK. Servo simulator panel pitch coil switch to fault. Box 2 engaged first. |
| 17B | Same as 17A but In AL.ARM | | | 0000<br>0000 | 0000<br>0000 | | | 0000<br>0000 | 0000<br>0000 | Both barhandles dropped. |
| 17B | Rerun | | | | | | | | | On 3rd retry,only affected channel disengaged, no dual at A/L TRK. |
| 17C | Same as 17A, but In AL.TRK above 150 Ft. | | | | | | | | | Affected FCC disengaged, No dual |
| 17D | Same as 17A, but In AL.TRK below 150 Ft. | | | | | | | | | Affected FCC disengaged, No dual not indicated. |
| 18A | Pitch Servo Coil Current Ramp Up Inbound | | | | | | | | | Affected channel disengaged, No dual at A/L.TRK |
| 19A | Roll Servo Discrete Open Inbound | | | | | | | | | |
| 19B | Same as 19A but In AL.ARM | | | | | | | | | Affected barhandle dropped; No dual indicated. |
| 19C | Same as 19A but In AL.TRK above 150 Ft. | | | | | | | | | Affected barhandle dropped, No dual indicated. |
| 19D | Same as 19A but In AL.TRK below 150 Ft. | | | | | | | | | Affected barhandle dropped; No dual not indicated. |

| | | Pin | | Open Pin Faults |
|---|---|---|---|---|
| Case | Circuit | No. | Function | |
| 20a | CU18<br>2901 No.3<br>(data bits<br>8 11) | 24 | Data<br>Input<br>Bit 1 | Upon opening, both FCC's disengaged. NORMAL-STANDBY switch was in STANDBY. |
| 20 | | 11 | F = 0 | Faulted FCC disengaged. SPLIT and NO DUAL annunciated. Faulted pin transmits signal to the status register. |
| 20b | | 4 | Address<br>bit $A_0$ | Faulted FCC disengaged. SPLIT, NO DUAL, and NO ALIGN annunciated at initiation of AL TRK. |
| 20c | | 17 | Address<br>bit $B_0$ | Both FCC's disengaged. AP DISC and SPLIT annunciated. |
| 20d | | 37 | Data<br>Output<br>bit 1 | Faulted FCC disengaged. AP DISC and SPLIT annunciated on disengagement. NO DUAL annunciated at AL TRK. |
| 21 | CU16 | 1 | | Fault had no effect on computer operation. Pin used only in reset of stack vector and transfer bus access control registers. |
| 22a | CU10<br>Control<br>Register<br>29LS18 | 1 | Data<br>Input<br>bit 0 | Faulted FCC disengaged. NO DUAL, NO ALIGN, and SPLIT annunciated. Pin 1 is coupled to Pin 2 (CR35, see fault following) and, when the next address control prom sets OE low, to direct input bit D1 of microprogram sequencer CU14. |
| 22b | | 2 | Data<br>Output<br>bit $Q_0$ | Faulted FCC disengaged. SPLIT, NO DUAL annunciated. Faulted bit drives control line CR35, which is address bit A3 of the 2901's when the processor address multiplexer couples CR35 to address line A03. |
| 22c | | 10 | Data<br>Output<br>bit Y2 | Faulted FCC disengaged. SPLIT, NO DUAL, and NO ALIGN annunciated. Faulted pin is direct input bit D3 to microprogram sequencer CU15 when bit D3 is not being controlled by instruction mapper prom CU7. In turn, CU15 outputs this bit as address bit A7 to the control store proms when CU1E is in direct address mode. |

| Case | Circuit | Pin No. | Pin Function | Open Pin Faults |
|---|---|---|---|---|
| 22e | CU10 | 4 | Data Input bit D1 | Faulted FCC disengaged; other FCC went to CWS. CMD DISC annunciated. Control line CR14 is latched to bit D1 on rising clock pulse, and when next address control prom sets OE low, to direct input bit DO of microprogram sequencer CU14. When selected by data select multiplexer DU28, CR14 is used as data bit DO6. |
| 22c | | 4 | | In a repeat of previous case, faulted FCC disengaged. Other FCC stayed in CMD. SPLIT and NO DUAL annunciated. |
| 22f | | 12 | Data Input bit D2 | Faulted FCC disengaged, other FCC stayed in CMD. NO DUAL and SPLIT annunciated. Control line CR33 is latched to Pin 12 on rising clock pulse. CR33 is used as processor A address bit AP1 when connected by the A address multiplexer. Also, CR33 can be coupled to processor input data bit DO5 by data select multiplexer DU21. |
| 23a | CU15 Micro-program Sequencer 2911 | 9 | Not Zero | Faulted FCC disengaged. SPLIT and NO DUAL annunciated at ALIGN point in landing. Pin 9 forces all outputs of CU15 to zero when it is low. Open pin prevented HI signal from control register CU21 from reaching CU15, zeroing all outputs and causing erroneous address to control store memory. |
| 23b | | 19 | Not FE | Faulted FCC disengaged. Processor halted. System failed to capture glide slope. The FE signal is one of four used to control the operation of the 2911 micro program sequencer. In most combinations of the signals, the absence of the FE signal causes a push or pop of a counter stack in addition to a jump. |
| 23c | | 19 | Not FE | Repeat of previous fault. Faulted FCC disengaged. Other FCC stayed in CMD. SPLIT and NO DUAL annunciated. |
| 23d | | 20 | PUP | Faulted FCC disengaged. NO DUAL and SPLIT annunciated. PUP is Push/Pop control signal. Open pin prevents pushing the microprogram counter contents onto the internal stack. |

|  |  | Pin |  |  |
|---|---|---|---|---|
| Case | Circuit | No. | Function | Open Pin Faults |
| 23e | CU15<br>Microprogram<br>Sequencer<br>2911 | 10 | S0<br>Address<br>Source<br>Selection<br>Control | Faulted FCC disengaged. NO DUAL and SPLIT annunciated. S0 is one of the four signals used in selecting the source of the next address. S0 open generally results in wrong source producing a jump to the wrong address. |
| 23f |  | 5 | D2<br>Direct<br>Input<br>bit D2 | Faulted FCC disengaged. NO DUAL and SPLIT annunciated. D2 is one of four bits which can be selected as the output of the 2911. Fault would cause the wrong control store memory address on selection of direct input when the bit should be high. |
| 23g |  | 15 | Y3<br>Output<br>bit | Faulted FCC disengaged. NO DUAL and SPLIT annunciated. Y3 is one of four output bits of the 2911. This bit being open causes the wrong microinstruction to be selected whenever this bit should be high. |

| Case | Circuit | Pin No. | Pin Function | Grounded Pin Faults |
|---|---|---|---|---|
| 24 | C02<br>Hex<br>Inverter | 8 | Inverter<br>Output | Faulted FCC disengaged. Processor stopped. This signal fans out to several points, including NAND gate CU35C, which outputs the Read Enable signal to the data bus transceivers. NAND output is stuck high so that processor cannot read the CAPS data bus. |
| 25 | CU36<br>Quad. NOR<br>Gate | 4 | Gate<br>Output | Faulted FCC disengaged. NO ALIGN, SPLIT, and NO DUAL annunciated. Faulted pin being stuck low results in NAND gate U35A being stuck high, disabling the data bus transceivers from writing on the CAPS data bus. |
| 26 | CU28<br>Quad. NAND<br>Gate | 3 | Gate<br>Output | Faulted FCC disengaged. NO ALIGN, SPLIT, and NO DUAL annunciated. Processor stopped. Fault results in BKOF being stuck high, so that processor cannot access CAPS bus. Also, all interrupt inputs to the interrupt controller are set high. |
| 27 | CU36<br>Quad. NOR<br>Gate | 13 | Gate<br>Output | Faulted FCC disengaged. NO ALIGN, SPLIT, and NO DUAL annunciated. Processor stopped. Fault results in the processor being unable to transmit XAKF (transfer acknowledge) on the CAPS control bus. XAKF is stuck high. |
| 28 | D02<br>Shift/<br>Rotate<br>Multi-<br>plexer | 2 | Control<br>Input | Faulted FCC disengaged. SPLIT, NO ALIGN, NO DUAL annunciated. Faulted processor stopped. Fault causes wrong data to be inserted into microprocessor in some shift operations. |
|  |  | 14 | Control<br>Input | Faulted FCC disengaged. Fault causes wrong data to be inserted into microprocessors during some shift operations. |

## Grounded Pin Faults

| Case | Circuit | Pin No. | Pin Function |
|---|---|---|---|
| 29 | DU17<br>Micro-<br>processor | 36 | Y00 |
| | | 37 | Y01 |
| | | 38 | Y02 |
| | | 39 | Y03 |
| 30 | DU14<br>Micro-<br>processor | 36 | Y04 |
| | | 37 | Y05 |
| | | 38 | Y06 |
| | | 39 | Y07 |
| 31 | DH18<br>Micro-<br>processor | 36 | Y08 |
| | | 37 | Y09 |
| | | 38 | Y10 |
| | | 39 | Y11 |
| 32 | DH15<br>Micro<br>processor | 36 | Y12 |
| | | 37 | Y13 |
| | | 38 | Y14 |
| | | 39 | Y15 |

In each case, the faulted FCC disengaged. The faulted processor halted immediately. The y pins are the processor output pins for computed data. Under certain conditions, processor output is a memory address which is connected to the CAPS address bus, rather than data. Corruption of addresses is apparently the cause of the immediate processor halts

|  |  | Pin |  |  |
|---|---|---|---|---|
| Case | Circuit | No. | Function | Grounded Pin Faults |
| 33 | DH17<br>Micro-<br>processor | 32 | G | Faulted FCC disengaged. Faulted processor halted immediately. |
|  |  | 35 | $\bar{P}$ |  |
| 34 | DH14<br>Micro-<br>processor | 32 | G |  |
|  |  | 35 | $\bar{P}$ |  |
| 35 | DH18<br>Micro-<br>processor | 35 | P |  |
| 36 | DH16<br>Interrupt<br>Controller<br>2914 | 16 | V2 | Faulted FCC disengaged. Faulted processor stopped immediately. V2 is the most significant bit of the interrupt vector output of the 2914. This bit is also address bit A02 of the CAPS address bus when the vector output is enabled, and is hard-wired to address line A02. |
| 37 |  | 17 | V1 | Faulted FCC disengaged. Faulted processor stopped immediately. V1 is the middle bit of the three-bit interrupt vector of the 2914. This pin is hard wired to CAPS address bus line A01. |
| 38 |  | 18 | V0 | Faulted FCC disengage. Faulted processor stopped immediately. V0 is the least significant bit of the interrupt vector output of the 2914. This pin is hard-wired to CAPS address bus line A00. |
| 39 |  | 28 | I0 | Faulted FCC disengaged. Faulted processor stopped immediately. I0 is a micro-instruction bit to the 2914. |
| 40 |  | 31 | I1 | Faulted FCC disengaged. Faulted processor stopped immediately. I1 is a micro-instruction bit to 2914. |
| 41 |  | 32 | I2 | Faulted FCC disengaged. Faulted processor stopped immediately. I2 is a micro-instruction bit to the 2914. |

## GROUNDED PIN FAULTS

| Case | Circuit | Pin No. | Pin Function | |
|---|---|---|---|---|
| 42a | DU16 Interrupt Controller 2914 | 34 | Instruction Enable | Faulted FCC disengaged. Faulted processor halted. Pin 34 is a logic-low instruction enable which should only go low when the instruction lines I0-I3 have been set. The pin stuck low causes the 2914 to read erroneous instructions. |
| 42b | | 26 | P4 Interrupt Request | Faulted FCC disengaged. Faulted processor halted. Pin 34 is a logic-low interrupt request. With the fault inserted, an interrupt request at priority 4 is generated whenever the corresponding mask bit is not set and a higher priority unmasked interrupt is not present. |
| 42c | | 39 | P2 Interrupt Request | Faulted FCC disengaged. Faulted processor halted. This is the same situation as in the previous case, except at a lower priority level. |
| 42d | | 20 | P7 Interrupt Request | Faulted FCC disengaged. Faulted processor halted. This is the same situation as in the previous two cases, except at the highest priority level. |
| 42e | | 25 | M4 Mash Bit | Faulted FCC disengaged. Faulted processor halted. This fault prevents priority Level 4 interrupts from being masked. |
| 42f | | 19 | M7 Mask Bit | Faulted FCC disengaged. Faulted processor halted. This fault prevents highest priority interrupts from being masked. |

| | | | | | FCC #1 CTA WINDOW | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | A1 | A2 | A3 | A4 | B1 | B2 | B3 | B4 | |
| CASE | ADDRESS VARIABLE | | | AP. ONE<br>FAIL | AP.TWO<br>FAIL | | | | | |
| | STRIP CHNL | | | 3635 | 3634 | | | | | |
| 43 | Open Roll Gyros 1 & 2 in AL.ARM | | | 0000<br>0001 | 0000<br>0001<br>0000 | | | | | Disconnected on Second Fault. 3634 flashed 0001 before reverting to 0000. |
| 44 | Open roll Gyros 1 & 3 to FCC #1 in AL.ARM | | | | | | | | | Sensors 2 & 3 still valid into box 2. No disconnect; No dual at AL.TRK. |
| 45 | Ramp Up Vert. Gyro #1 in APP; Open Vert. Gyro #2 in AL.ARM | | | | | | | | | Two sensors lost; both boxes disengaged. |

# BIBLIOGRAPHY

AC 25, 1309-1, System Design Analysis, Federal Aviation Administration, September 7, 1982.

AC 120-28C, Criteria for Approval of Category III Landing Weather Minima, Federal Aviation Administration, March 9, 1984.

Bjurman, B. E., et al., Airborne Advanced Reconfigurable Computer System (ARCS), NASA-CR-145024, Prepared for Langley Research Center, NASA by Boeing Commercial Airplane Company under contract NAS1-13654, August 1976.

Conn, R. B., et al, "CAST - A Complementary Analytic - Simulative Technique for Modeling Complex, Fault-Tolerant Computing Systems," AIAA Computers in Aerospace Conference, Los Angeles, California, November 1977.

DOT/FAA/CT-82/140, Digital Flight Control System Validation Technology Assessment, July 1982.

DOT/FAA/CT-82/154, Integrated Assurance Assessment of a Reconfigurable Digital Flight Control System, Volume I, April 1983.

Hitt, E. and D. Eldredge., "A Review and Application of Analytical Models in Fault Tolerant Avionics Validation," Proceedings of IEEE/AIAA 5th Digital Avionics Systems Conference, Fall 1983.

Karlin, S., A First Course in Stochastic Processes, Academic Press, 1966.

Lockheed-Georgia Company Engineering Report LG81E0126, Simulator Investigation Plan for Digital Flight Controls Validation Technology, as revised 10 April 1981.

MIL-M-38510, Microcircuits, General Specification for.

Military Standardization Handbook 217C, Reliability Prediction of Electronic Equipment, United States Air Force, Rome Air Development Center, 9 April 1979, with Notice 1, Supplement, 1 May 1980.

MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis.

Mulcare, D. B., et al., Industry Perspective on Simulation Methods for Validation and Failure Effects Analysis of Digital Flight Control Avionics, NASA CR-152234, Moffett Field, California, February 1979.

NASA RDFCS System Interface Document, April 8, 1981.

NASA Report prepared for Langley Research Center by Raytheon Company, Contract NAS1-12668, Reliability Model Derivation of a Fault-Tolerant, Dual, Spare-Switching Digital Computer System, March 1974.

Ng, Y. W., and A. Avizienis., ARIES 76 User's Guide, National Science Foundation Report No. NSF-MCS-7203633-78944, University of California, Los Angeles, Report No. UCLA-ENG-7894, December 1978.

Nuclear Regulatory Commission Report NUREG-0492, Fault Tree Handbook.

RTCA Document DO-178, Software Considerations in Airborne Systems and Equipment Certification, November 1981.

# ACRONYMS AND ABBREVIATIONS

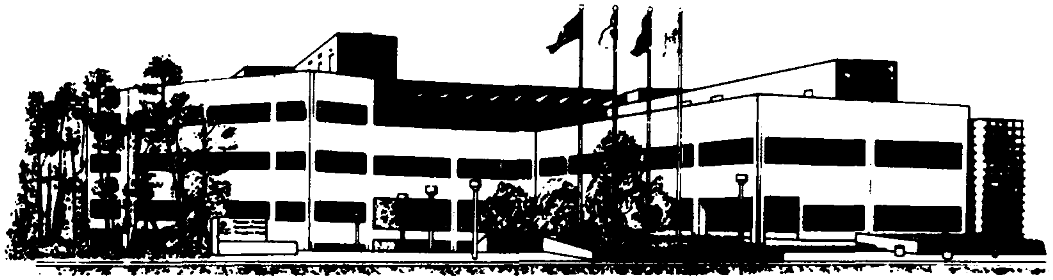
| | |
|---|---|
| A/L | Approach/Land |
| AC | Alternating Current |
| AC | Advisory Circular |
| ADI | Automatic Direction Indicator |
| ALU | Arithmetic Logic Unit |
| ARIES | Automated Reliability Interactive Estimation System |
| ARINC | Aeronautical Radio Incorporated |
| CAPS | Computer Aided Production Simulator |
| CAST | Complementary Analytic Simulative Technique |
| CARE | Computer Aided Reliability Evaluator |
| CARSRA | Computer-Aided Redundant System Reliability Analysis |
| CTA | CAPS Test Adapter |
| DFCS | Digital Flight Control System |
| DOT | Department of Transportation |
| DSP | Discrete Switch Panel |
| EFMA | Executive Failure My A |
| EFMB | Executive Failure My B |
| EFOA | Executive Failure Other A |
| EFOB | Executive Failure Other B |
| EFW | Executive Failure Word |
| FAA | Federal Aviation Administration |
| FAR | Federal Acquisition Regulation |
| FCC | Flight Control Computer |
| FMEA | Failure Mode and Effect Analysis |
| HSI | Horizontal Situation Indicator |
| Hz | Hertz |
| IAA | Integrated Assurance Assessment |
| IC | Integrated Circuit |
| ILS | Instrument Landing System |
| LVDT | Linear Voltage Differential Transducer |
| mA | Milliampere |
| MDICU | Modular Digital Interface Control Unit |
| NA | Normal Accelerometers |
| NASA | National Aeronautics and Space Administration |
| PROM | Programmable Read-Only Memory |
| RAM | Random Access Memory |
| RBDCP | Reliability Block Diagram Computer Program |
| RDFCS | Redundant Digital Flight Control System |
| REL | Reliability |
| REL COMP | Reliability Computers |
| RTCA | Radio Technical Commission for Aeronautics |
| SSP | Servo Simulation Panel |
| TASRA | Tree Aided System Reliability Analysis |
| WAI | Warning Annunciation Indicator |
| XMTR | Transmitter |

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 4
## QUADRUPLEX DIGITAL FLIGHT CONTROL SYSTEMS



**PREPARED BY:**

**COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070**

**PREPARED FOR:**

**FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405**

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# TABLE OF CONTENTS

Section | Page

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

# 1. INTRODUCTION

The purpose of this chapter is to provide background information pertinent to assurance assessments of quadruplex Digital Flight Control Systems (DFCS). to identify and discuss some of the current problems associated with assurance assessments, and to present related evaluation approaches and techniques.

Assurance assessment is a collective phrase that covers design correctness, system verification, and system validation. By ensuring that a proposed system functions according to design specifications, assurance assessments serve as tracking guidelines during system development.

The material contained in this chapter relies heavily on the development and validation of a double fail-operational DFCS architecture reported in Quadruplex Digital Flight Control Assessment, DOT/FAA/CT-86/30 (D. B. Mulcare, L. E. Downing, and M. K. Smith). This report serves as the basis for this presentation, and generous use has been made of its data, text, and illustrations.

# 2. BACKGROUND

The first DFCSs were introduced in the mid-1970s. They used fairly conventional architectures and were largely copies of prior analog systems. These systems used parallel replicated lanes with sensors fanning into the processors, which in turn fanned out to actuators or displays. Figure 2-1 shows an expansion of this architecture for the pitch-axis of an Augmented Fly-By-Wire (AFBW) function. Except for cross-channel communication, all signal paths are dedicated analog paths. Fan-in is minimized by having one set of sensors feed directly into each computational channel. In figure 2-1, each channel broadcasts its received sensor inputs to the other three channels.

These early Flight Control Systems (FCS) were flight-critical for a very limited time (e.g., autoland). By 1975, the Federal Aviation Administration (FAA) recognized the trend from analog systems to their digital implementations. The FAA also recognized the challenges that would accompany this transition to a new technology (Reed and Boothe, 1977). More recently, the FAA has identified a need to become familiar with the emerging full-time, full-authority, "flight-critical" fly-by-wire/light systems (Larsen and Carro, 1986). Besides the functional criticality of the systems, the concepts of envelope limiting, flying-qualities management, and system reconfiguration without loss of redundancy during the processing of hard and soft faults (transparent recovery) have brought new issues to the forefront. As a result, new areas of concern have emerged as fault-tolerant systems come online.

Advanced systems become interdisciplinary as their complexity increases. The overall aspects of certification become more system-integrity oriented. As a result, there is a need to formulate a uniform approach to assurance assessments. From a reliability point of view, analytical assessments of critical functions are demanding and tedious. They include the evaluation of the dissimilar versions of hardware and software used in the various lanes of redundancy, the need for backup systems, faulted recovery techniques, status instrumentation, and pilot workload.

Quadruplex Digital Flight Control Assessment (D. B. Mulcare, L. E. Downing, and M. K. Smith) defines a double fail-operational DFCS that was designed, analyzed, implemented, and validated relative to system fault-tolerance (figures 2-2 and 2-3). In this chapter, a subset of the DFCS system, the pitch-axis control functions, will be used to demonstrate important portions of an integrated approach to assurance assessment. The system-level, fault-tolerant design was developed around an engineering development model of the L-1011 FCS and will be verified using a predicate/transition network simulation (Barton, Mulcare, and LeBlanc, AIAA Paper, 1985).

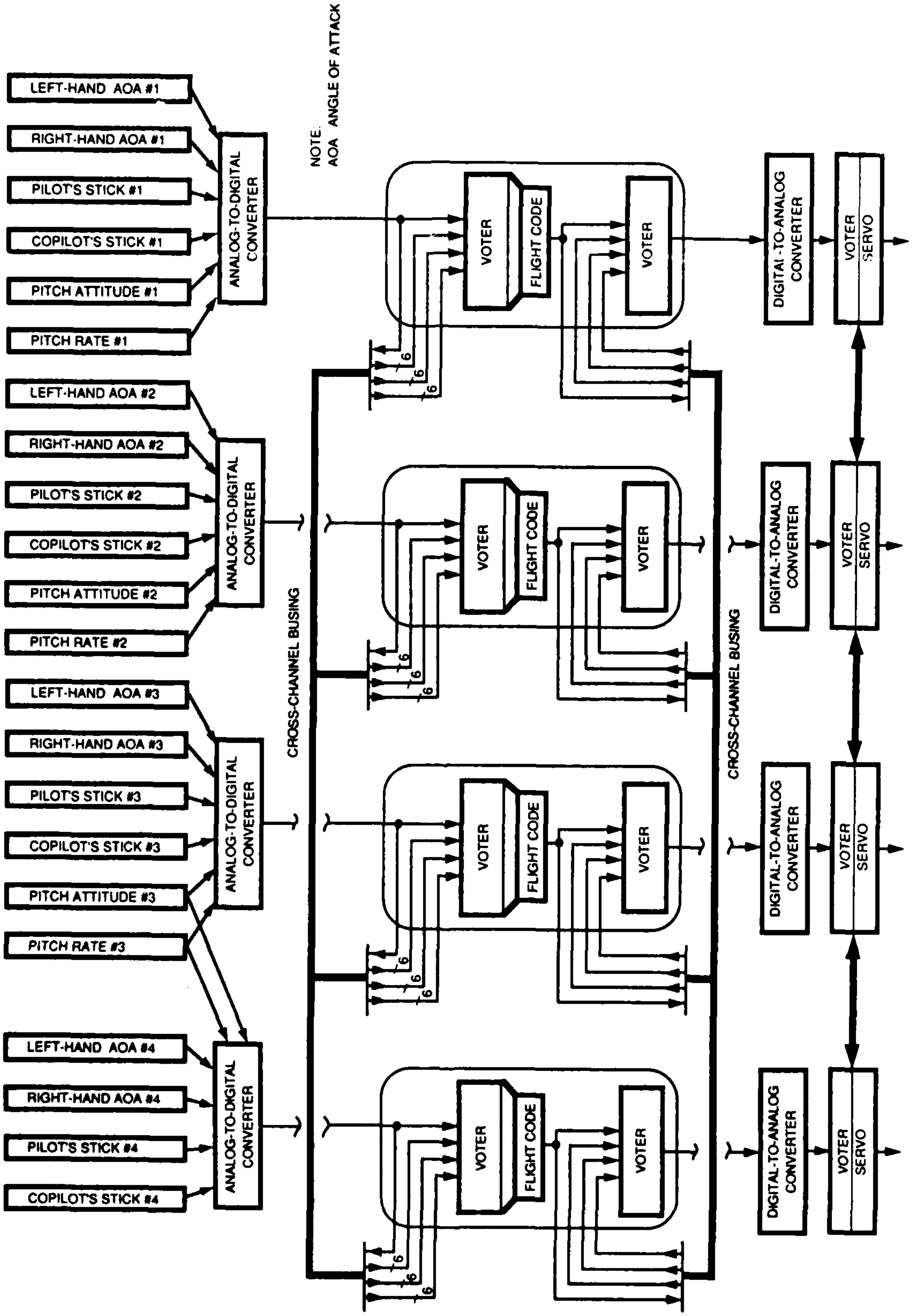


FIGURE 2-1. BASELINE SYSTEM ARCHITECTURE

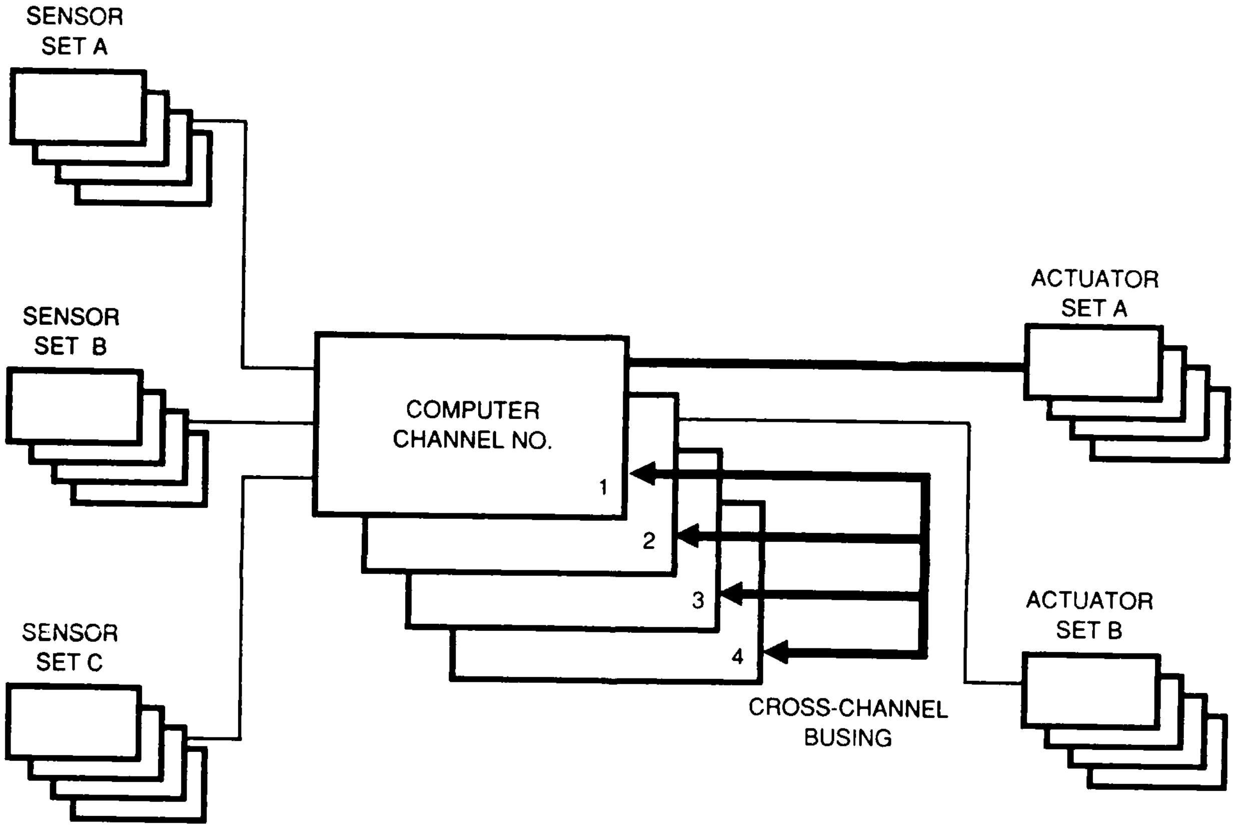


FIGURE 2-2. QUADRUPLEX DIGITAL FLIGHT CONTROL SYSTEM ARCHITECTURE

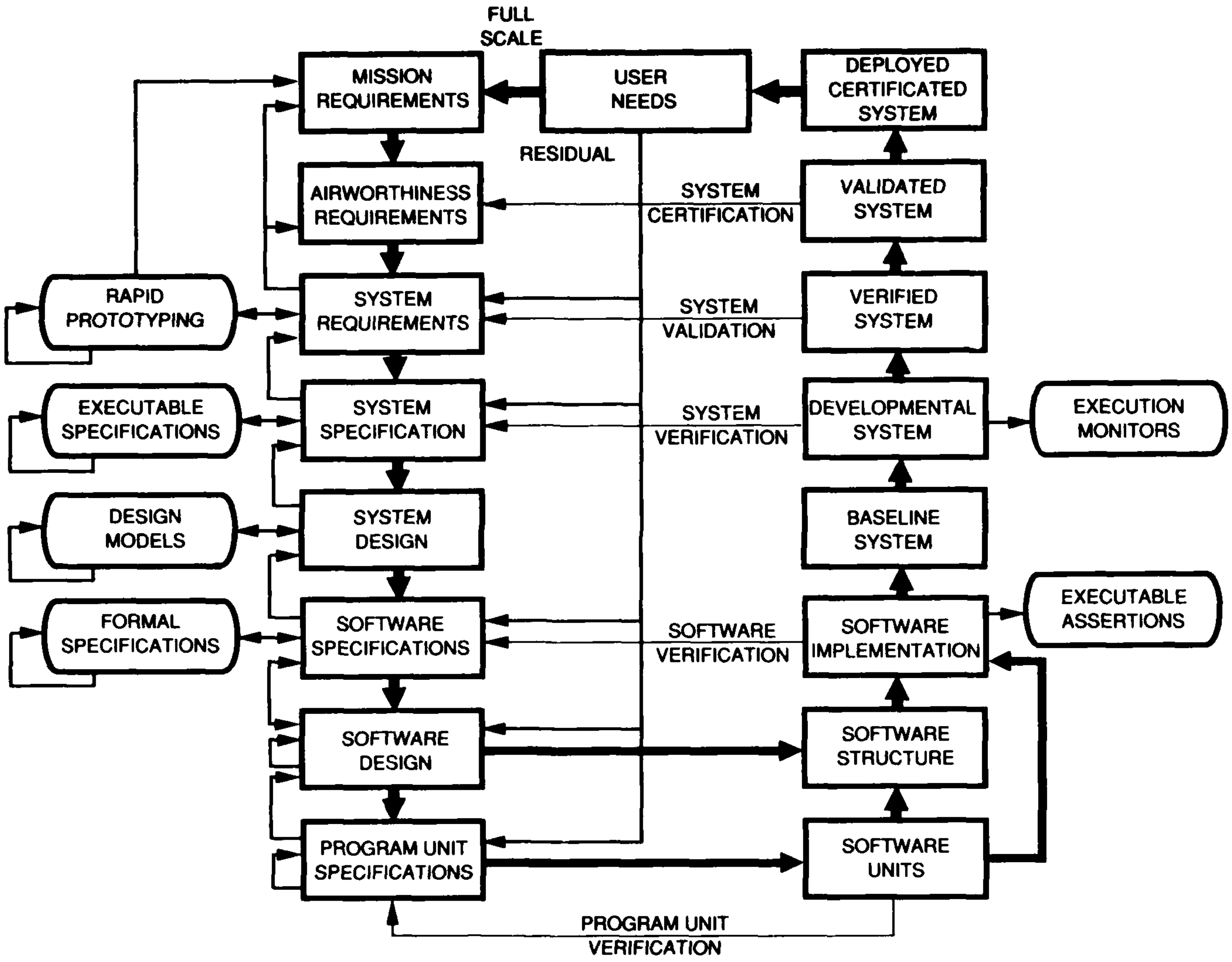


FIGURE 2-3. DIGITAL FLIGHT SYSTEM LIFE CYCLE

The data contained in this chapter havı been developed from the DFCS and systems simulator shown in figures 2-4 and 2-5. (This system was located at Ames Research Center, Moffett Field, California.) The original dual-dual architecture was transformed into a quadruplex architecture by making software changes that extended the fault-tolerance capability to full-time flight-critical operation. The resulting implementation was not optimal for flight application, but it worked well for demonstrating a verified design and served to illustrate the integrated assurance methodology necessary throughout the development process for flight-critical applications.

With the introduction of full-time flight-critical control functions, substantially more effort must be directed toward guaranteeing airworthiness than was necessary for flight-phase critical functions. A tremendous increase in system complexity has also been incurred with (1) the advent of fault-tolerant (error-correcting) architectures, (2) the myriad assurance tools necessary to confirm system airworthiness, and (3) digital implementation. To attain requisite airworthiness of the flight-critical control system, lower levels of digital implementation must be examined. An integrated assurance methodology is essential for compliance with the provisions of AC 25.1309.1.

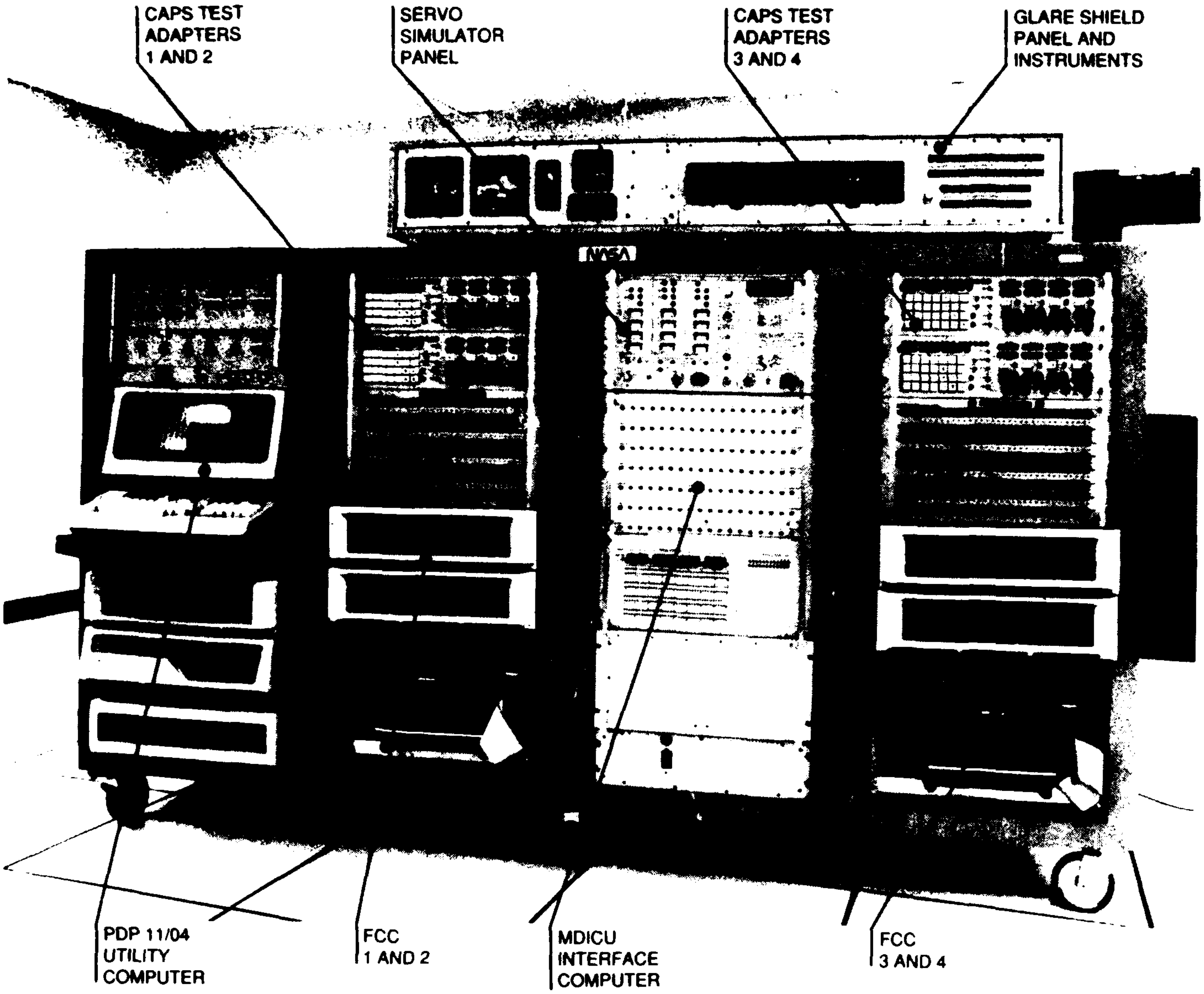
The assurance tools and methods required for use with these advanced systems have not been fully developed. It is not clear that their use ensures that the required level of reliability is achieved. In civil aircraft, current reliability levels are set at $10^{-9}$ or less.

In a comprehensive assessment process, several dimensions of an integrated assurance method should be reviewed and acknowledged. These dimensions include the performance, analysis, testing, and inspection of reliability analyses, failure effects analyses, simulation and functional performance assessment methods. The integration assurance methodology is shown in figure 2-6. Analysis is the dominant method for reaching high levels of assurance in the early development of an FCS, particularly when only models or abstractions are available. At this stage, a systems walk-through can be especially valuable.

Analysis forms the basis of conclusive testing. It must be accomplished at various stages of the development process to maximize the effectiveness of testing, as shown in figure 2-7. Testing based on proper analysis assures the system designer that the implementation is in accord with design specifications and requirements. The coincident application of various test cases derived through analysis provides an increased level of confidence in the correctness of the design and its implementation.

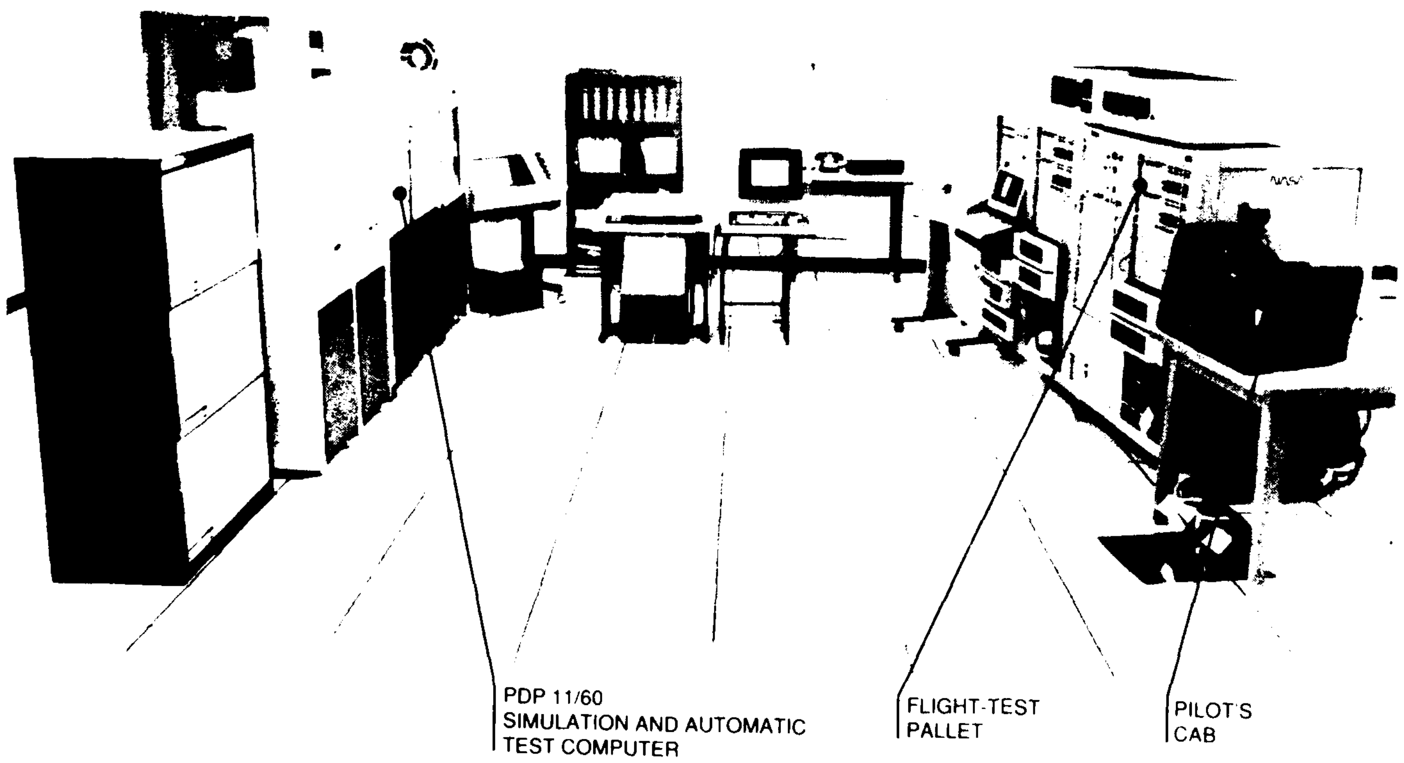
An integrated approach to proving implementation correctness is essential because testing can only be applied to the actual article. Testing primarily examines the validity of analytical results and the underlying assumptions.

The assessment methods presented are not necessarily the best or only techniques for every flight-critical DFCS use. The methods do, however, provide a representative example of the airworthiness assurance of the full-time, flight-critical DFCSs that will be making their appearances in the near future. Although the pitch-axis example discussed here is scaled, it is representative of the challenges in certifying double fail-operational quadruplex DFCSs.


CAPS TEST ADAPTERS 1 AND 2
SERVO SIMULATOR PANEL
CAPS TEST ADAPTERS 3 AND 4
GLARE SHIELD PANEL AND INSTRUMENTS
NASA
PDP 11/04 UTILITY COMPUTER
FCC 1 AND 2
MDICU INTERFACE COMPUTER
FCC 3 AND 4

**(a) Flight-test Pallet**

FIGURE 2-4. RECONFIGURABLE DIGITAL FLIGHT CONTROL SYSTEM FACILITY SETUP (FLIGHT TEST PALLET)



**(b) Simulation Setup**

FIGURE 2-5. RECONFIGURABLE DIGITAL FLIGHT CONTROL SYSTEM FACILITY SETUP (SIMULATION SETUP)

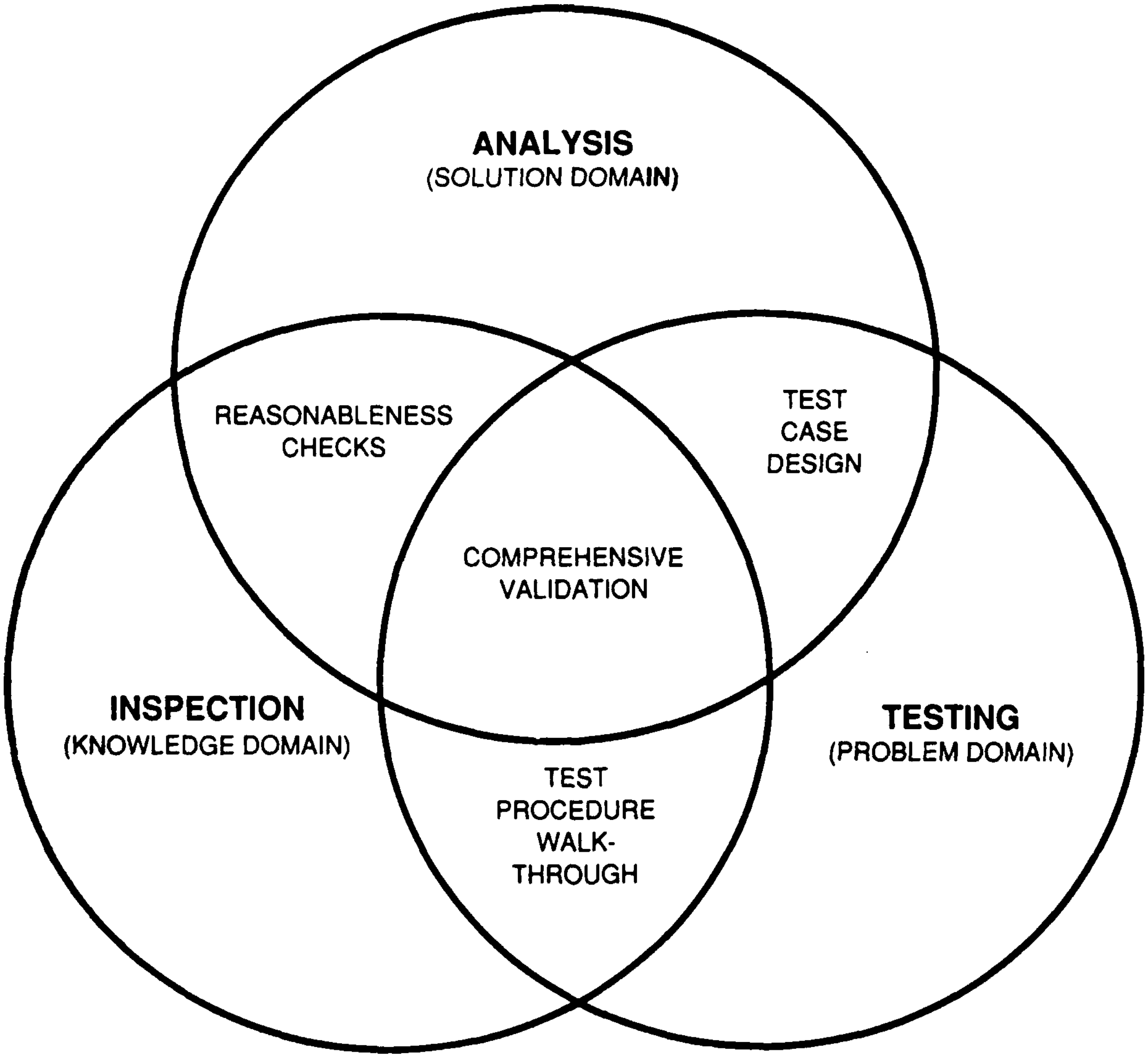


FIGURE 2-6. INTERDEPENDENCE OF ASSURANCE METHODS

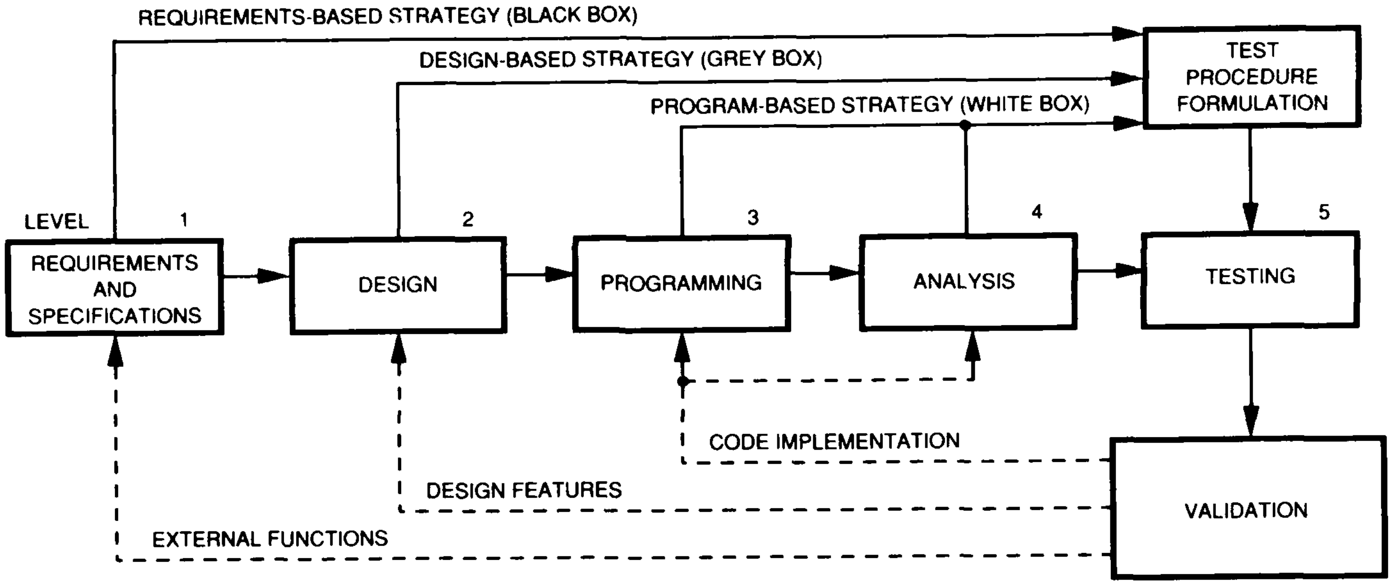

REQUIREMENTS-BASED STRATEGY (BLACK BOX)
DESIGN-BASED STRATEGY (GREY BOX)
PROGRAM-BASED STRATEGY (WHITE BOX)
TEST PROCEDURE FORMULATION
LEVEL
1
2
3
4
5
REQUIREMENTS AND SPECIFICATIONS
DESIGN
PROGRAMMING
ANALYSIS
TESTING
CODE IMPLEMENTATION
DESIGN FEATURES
EXTERNAL FUNCTIONS
VALIDATION

FIGURE 2-7. MULTILEVEL TESTING

There is a considerable difference in the airworthiness demands for a full-time flight-critical system or function and a flight-phase critical function. The increased demands for airworthiness assurances are primarily a function of system exposure time (the time from last system validation to completion of the present use). When a flight-critical function is implemented digitally, there is concern about the capability of ensuring its airworthiness. Therefore, these examples seek to demonstrate the requisite technology and its application in a representative DFCS development program for a pitch-axis augmented fly-by-wire/light system.

# 3. THE ASSURANCE ASSESSMENT PLAN

The FAA AC 25.1309-1 recommends procedures for demonstrating compliance with the requirements of Part 25 of the Federal Aviation Regulations (FAR) for flight-essential and flight-critical avionics systems. This publication outlines the use of a quantitative safety analysis that may include probability analysis, fault tree analysis, failure-modes and effects analysis, and other comparable techniques such as systems simulation. Such an integrated approach is discussed in detail in Ness, 1983 and chapter 3 of this handbook. This chapter describes a system-level failure-effects simulation that focuses on flying-qualities degradation and real-time multilevel assessment of software behavior stressing architectural fault tolerance.

The flying-qualities degradation testing is a conventional technique and incorporates an all-up simulation including sensors, servos, research cockpit pilot interface, aircraft model, and test electronics. The real-time multilevel testing is a considerably more sophisticated technique and a valuable new testing methodology for flight-critical systems. This approach to multilevel demonstration testing is a means of establishing high levels of confidence in the airworthiness of a given flight-critical DFCS.

Figures 2-3 and 3-1 present the developmental activities and expected results for a verification and validation process as it relates to a digital flight system design. Table 3-1 indicates five typical levels of testing that might be undertaken. The top level, most generally seen, is conventional system functional testing. Later on in this chapter the flying qualities for a Relaxed Static Stability (RSS) airplane test case are examined. Multilevel control structures that were also related to simulation developmental activities are examined coincidentally, as shown in figure 3-2. To conclusively examine sophisticated flight-critical systems requires that significant emphasis be placed on automated testing and wideband instrumentation. This level of testing is illustrated in table 3-1.

One major aspect of flight-critical DFCS verification and validation is the verification that logic for the top-level systems using fault-tolerant architecture has been implemented. Other testing might check the design and the redundancy of the design verification channel, because fault-tolerant architectures demand intricate hardware and software logic to maintain cross-channel coordination.

This kind of verification testing occurs in the latter stages of system development and is addressed using the fidelity of an all-up FCS simulator. If the test simulator lacks an automated test capability that would permit other than system-level checks, then it is necessary to develop real-time test programs running in parallel (commonly known as real-time test monitors). Real-time test monitors are extremely valuable in achieving the necessary level of assurance. Figure 3-3 presents the components of an all-up simulation facility (the

Reconfigurable Digital Flight Control System (RDFCS) Facility at Ames Research Center), and table 3-2 highlights some of the more significant capabilities of that facility.

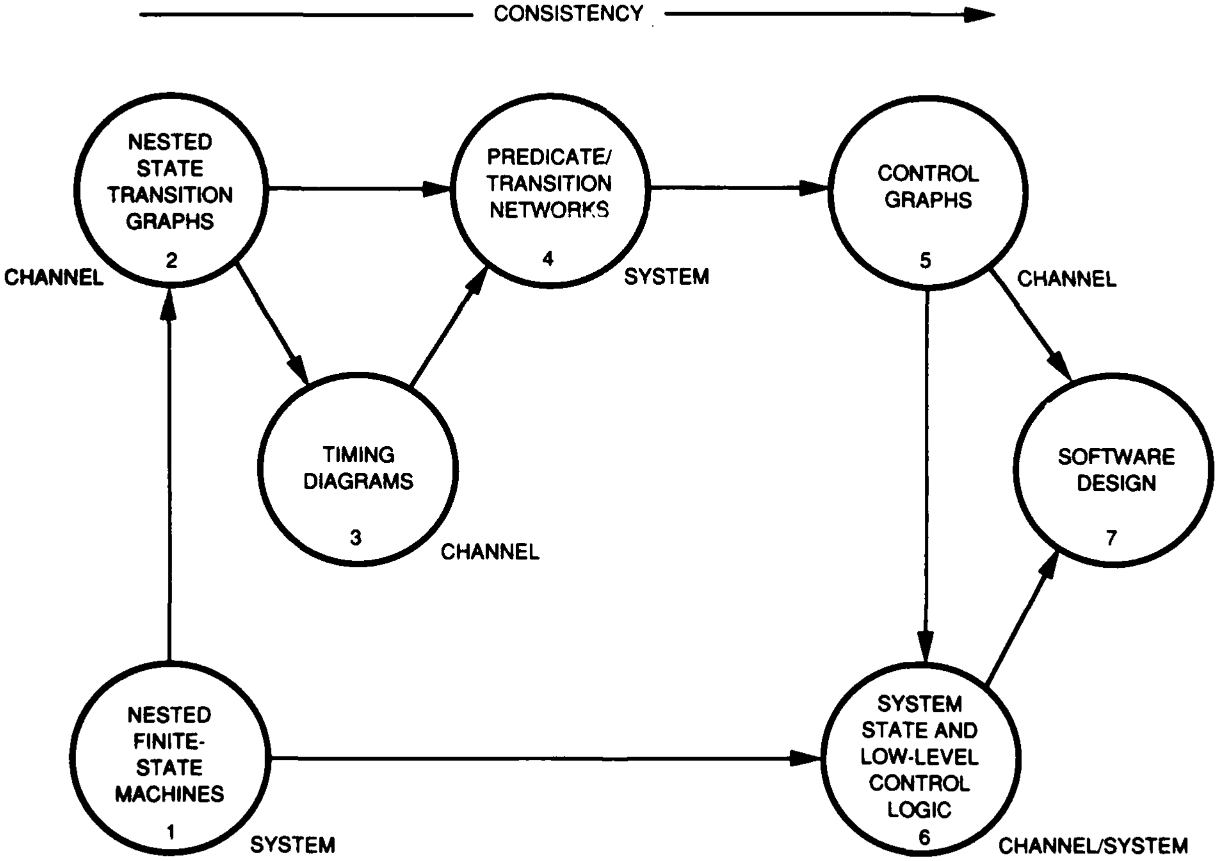

CONSISTENCY
NESTED STATE TRANSITION GRAPHS
2
CHANNEL
PREDICATE/ TRANSITION NETWORKS
4
SYSTEM
CONTROL GRAPHS
5
CHANNEL
TIMING DIAGRAMS
3
CHANNEL
SOFTWARE DESIGN
7
NESTED FINITE-STATE MACHINES
1
SYSTEM
SYSTEM STATE AND LOW-LEVEL CONTROL LOGIC
6
CHANNEL/SYSTEM

FIGURE 3-1. ARCHITECTURAL DESIGN TASKS

TABLE 3-1. DIGITAL FLIGHT CONTROL SYSTEM TESTING SCENARIO

| Type of Testing | Focus | Execution Monitor | Monitor Location | Primary Concern |
|---|---|---|---|---|
| System validation | System performance | None | N/A | Fault Flying qualities |
| System verification | System state | Nested finite-state machines | Simulation/ test computer | Faulted states |
| | Channel synchronization | Predicate/ transition network | Single channel | Single-point failures |
| | Mode/fault logic | Boolean expressions | Single channel | Logic correctness |
| | Control flow | Control graphs with assertions | Single channel | Path traversals |

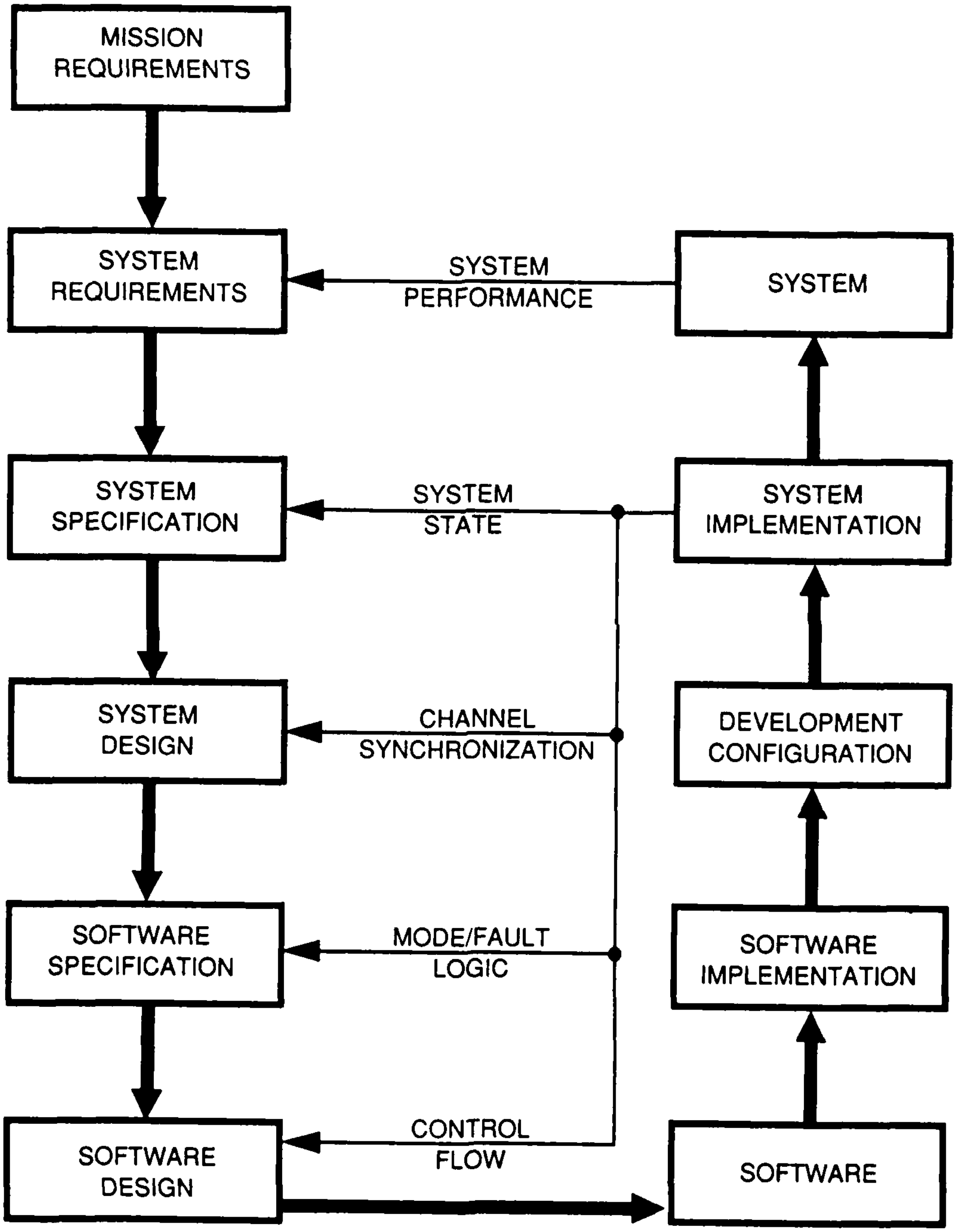


FIGURE 3-2. MULTILEVEL-TESTING CLOSURE

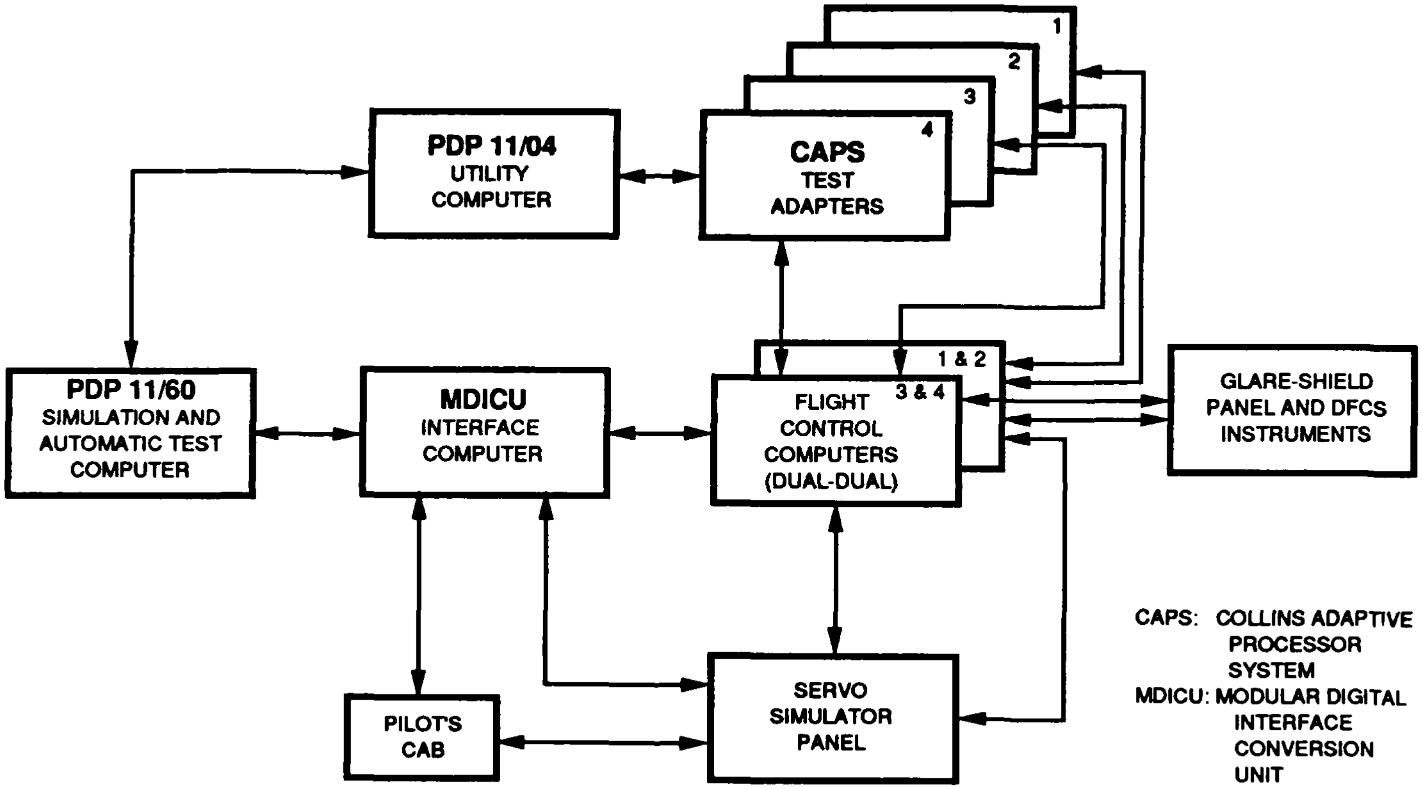


FIGURE 3-3. RECONFIGURABLE DIGITAL FLIGHT CONTROL SYSTEM ALL-UP SIMULATION COMPONENTS

TABLE 3-2. RECONFIGURABLE DIGITAL FLIGHT CONTROL SYSTEM FACILITY CAPABILITIES

| Feature | Significance/Elaboration |
|---|---|
| Language for FCCs and MDICU<br>Augmented higher order | Comprehensible, well composed software for DFCS or test purposes<br>Instruction set augmented for machine-related use<br>Mature support software |
| Efficient airframe simulation | 75 percent quiescent frame time at 50 Hz<br>Ample time for test software execution |
| Automated fault insertion | Simulated sensor faults in MDICU<br>Simulated FCC memory faults via PDP-11/04 laboratories<br>FCC hardware fault insertion via Draper |
| Software instrumentation | PDP-11/60 programmed data retrieval via the PDP-11/04 and Collins Adaptive Processor System (CAPS) test retrieval<br>Background mode FCC data retrieval<br>Data object access to all FCCs via link loader options |

# 4. THE USE OF SIMULATION AS AN ASSURANCE TOOL

Engineering-level systems components and a piloted simulation constitute a central and critical part of the DFCS development process. They are used during the verification and validation process of systems development. The work described here is intended to further demonstrate a more effective use of system simulation during the assurance process. For both piloted flight , and system simulators the importance of the use of actual system elements in providing the required fidelity cannot be overemphasized, particularly for the m, re complex digital systems. The final assessment of the performance of the control-system handling qualities, degraded systems operation, electronic displays, and side-arm controllers can only be made with a piloted simulator. In digital systems, performance can be seriously compromised as a result of the inherent phase lags that are induced into the system.

## 4.1. Assurance Assessment

Throughout the development of a product, assurance features must be designed to accommodate the verification and validation processes (Goldberg, 1979 and Wensley, 1969). As the complexity of the system increases, particularly in fault-tolerant designs, early planning for accountability is of utmost importance to guarantee the conclusiveness of the assurance process.

## 4.2. Digital Flight Control System Assurance Methodology

The quadruplex DFCS described by Mulcare, Downing, and Smith, 1987, was developed primarily by making software changes to a dual-dual DFCS flight-test pallet. Although constraints were imposed in the changeover from a dual-dual to a quadruplex setup, the resulting configuration was adequately representative of a conventional quadruplex system. Since the modification was originally developed to demonstrate rigorous system and software design methodologies (Mulcare, Ness, and Davis, 1984) the facility is well-suited for use as an assurance assessment demonstrator.

## 4.3. Simulation Development

Within the constraints of the existing dual-dual FCS, a representative fail-operational-squared (fail-operational/fail-operational) architecture has been defined. The redundancy management coordination of this design can be verified through predicate/transition network simulation, and the high-level software design is then represented in nested control graphs. Cross-channel coordination is effected through respective channel control states broadcast over serial digital buses. The system is then tested under various simulated faulted and abnormal conditions using real-time software execution monitors to resolve low-level system management events.

In the development of the simulator, RSS flight cases are used and validated, using airplane time-histories. New sensor outputs are routed through the Modular Digital Interface Conversion Unit (MDICU) to the flight computers. New mode and fault logic signals are assigned on the logic discrete switch panel on the FCS simulator. Lastly, the pitch-axis inputs are introduced into the flight computer by means of a manual control stick. It is therefore possible to assess flight-qualities degradation through real-time closed-loop systems simulation with or without pilot input.

FCS definition evolved in accordance with the development products shown in figure 2-3, which highlights the stages of mechanization along the downward path on the left of the figure and the assurance steps along the upward path on the right of the figure. Further details of the development activities are presented in table 4.3-1. In general, the objective is to highlight key steps corresponding to progressive system definitions that should lead to a certifiable DFCS. Design definition usually addresses either system functions or architecture. System-function definition centers on control laws, whereas system-architecture definition centers on system and software structure. It is particularly vital that the organization of the flight software be explicitly described prior to digital implementation. These aspects of system definition, particularly system/software architecture, are central to reliable/fault-tolerant DFCSs and will be further discussed before the presentation of application examples (see paragraph 4.6). These design tasks, noted in figure 3-1 are illustrated through a sequence of examples.

To assist in the design definition of a flight-critical FCS, an RSS airplane with a Fly-By-Wire (FBW) FCS is defined. The control law shown in figure 4.3-1 has been used in each of the four redundant FCS channels. Pilot command is through a control stick. Short-period damping is provided from the simulated airplane, and angle of attack (AOA) is used to control the pitch divergence that is associated with the relaxed static stability. Control-surface scheduling is used, because control-surface effectiveness increases with airspeed. Six point-mass simulation cases were used, as shown in table 4.3-2, with their sensor feedback gains.

## 4.4. Basic System Architecture

Channel redundancy for fault tolerance in DFCSs demands intricate hardware/software logic to maintain cross-channel coordination. Such wide bandwidth processes must take place dependably despite component tolerances, inaccuracies in timing, occasional software errors, and hardware faults. At risk are the integrity and continued proper operation of the total system. It is vital to confirm the safety and acceptability of the cross-channel logic under a broad range of deviant or discrepant conditions.

In the latter stages of system development, these concerns can be addressed using the fidelity of an all-up, real-time FCS simulator. However, such simulators do not usually incorporate the automated test capability that is necessary to permit checks at other than the system level. Real-time test programs are desirable; they run in parallel with redundant DFCSs to ascertain the correct cross-channel logic operation, thereby guaranteeing a high degree of resolution and certainty.

TABLE 4.3-1. DEVELOPMENT PHASE ACTIVITIES AND PRODUCTS

| | |
|---|---|
| 1. Conceptual Phase | |
| Purpose | Provide for user needs |
| Input | Mission requirements |
| Mech.* | Formulate system requirements; explore design solutions |
| Assur.* | Validate requirements; analyze design solutions |
| Product | System requirements and concepts |
| Status | Functional architecture; feasible design solution |
| 2. Definition Phase | |
| Purpose | Design for user needs |
| Input | Airworthiness and system requirements; system concepts |
| Mech.* | Formulate system specs; refine system concepts |
| Assur.* | Verify specs; validate system concepts |
| Product | System specs; conceptual system design |
| Status | Validated conceptual design; acceptable design solution |
| 3. Analysis Phase | |
| Purpose | Design system to specs |
| Input | System specs |
| Mech.* | Design system structure; design control laws |
| Assur.* | Verify software specs, system structure, and control laws |
| Product | System design; software and hardware specs |
| Status | Verified system structure; superior design solution |
| 4. Design Phase | |
| Purpose | Design software to specs |
| Input | Software specs |
| Mech.* | Design software structure; define software components |
| Assur.* | Verify software design and unit specs |
| Product | Software design; program unit specs |
| Status | Verified baseline design; comprehensive design definition |
| 5. Coding and Checkout Phase | |
| Purpose | Implement software to specs |
| Input | Unit specs |
| Mech.* | Implement program units |
| Assur.* | Check and debug units; verify program units |
| Product | Software implementation |
| Status | Baseline system config.; comprehensive system definition |

*NOTES: Mechanization process; Assurance process.

TABLE 4.3-1. DEVELOPMENT PHASE ACTIVITIES AND PRODUCTS (Continued)

| | |
|---|---|
| 6. Integration Phase | |
| Purpose | Construct system with hardware/software components |
| Input | Verified structure and components |
| Mech.* | Assemble/develop system |
| Assur.* | Identify and rectify inconsistencies |
| Product | System implementation |
| Status | Developmental system |
| 7. Development Test Phase | |
| Purpose | Test to spec requirements |
| Input | System specs |
| Mech.* | Develop system; optimize performance |
| Assur.* | Identify and rectify deficiencies; verify performance |
| Product | Verified implementation |
| Status | Verified system |
| 8. Validation Phase | |
| Purpose | Test for compliance with requirements |
| Input | System requirements |
| Mech.* | Modify system if necessary |
| Assur.* | Confirm acceptability |
| Product | Provisional configuration |
| Status | Validated system |
| 9. Certification | |
| Purpose | Demonstrate airworthiness compliance |
| Input | Airworthiness requirements and certification plan |
| Mech.* | Modify system if necessary |
| Assur.* | Confirm airworthiness |
| Product | Production configuration |
| Status | Certificated system |

*NOTES: Mechanization process; Assurance process.

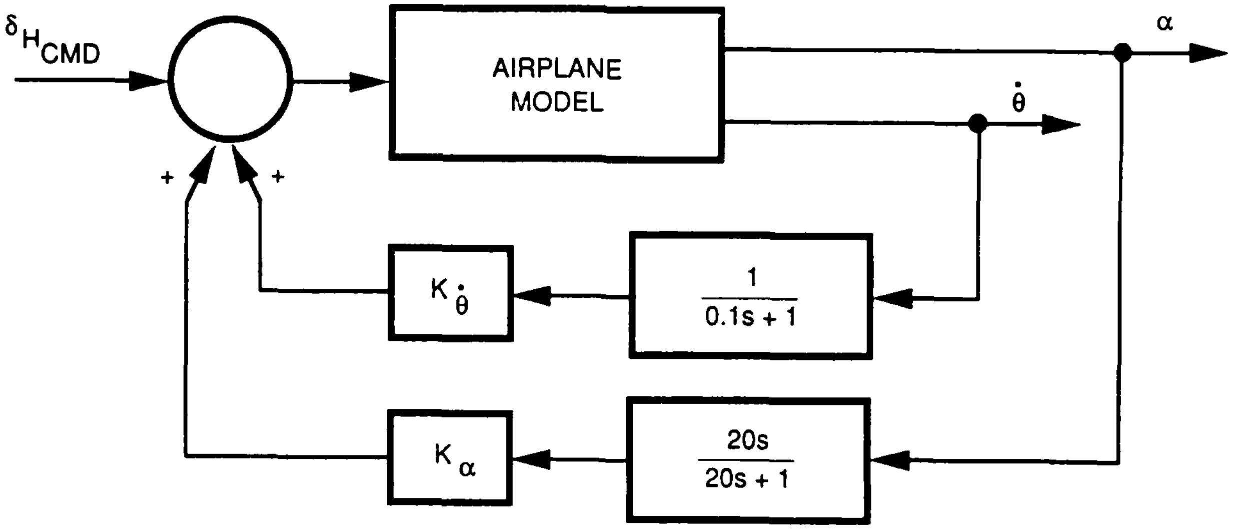


FIGURE 4.3-1. CONTROL LAW USED IN REDUNDANT FLIGHT CONTROL SYSTEM CHANNELS

TABLE 4.3-2. STABILITY AUGMENTATION GAIN SCHEDULING

| Flight | True | $K_\alpha$, | $K_{\dot{\theta}}$, |
|---|---|---|---|
| Case | Airspeed | deg/deg | deg/deg/sec |
| A1RSS | 283.7 | 1.00 | 0.70 |
| C13RSS | 910.7 | 0.73 | 0.10 |
| C15RSS | 442.2 | 1.00 | 0.40 |
| D2RSS | 487.1 | 1.00 | 0.33 |
| E3RSS | 265.7 | 1.00 | 0.80 |
| F6RSS | 224.1 | 1.00 | 0.50 |

## 4.5. Developing the Flight Control System

The top-level primary FCS requirements are assumed to be MIL-F-9490D operational states (Specification MIL-F-9490D). These requirements encompass both airplane flying qualities and system safety in terms of redundancy margins. Operation State 1 denotes normal system status and Level 1 flying qualities (good); State 2 allows some deterioration in safety margins and Level 2 flying qualities (somewhat degraded); State 3 indicates marginal safety and Level 3 flying qualities (marginal); and State 4 designates unsafe components or flying qualities (worse). Knowledge of flying-qualities degradation under conditions of successive component failures makes it possible to view the operational state logic from an architectural point of view. The system design task then focuses on defining the channel-level logic to effectuate the system-level logic.

Figure 4.5-1 represents the top-level DFCS channel logic design; the labels in the circles correspond to the particular states that can be assumed by the logic variables. These logic variables denote states or substates of the channel. The names appearing on the arcs of the state transition graphs designate independent logic events such as pilot-mode selection, timer interrupt, or component failure. Such events in turn may effect changes in the channel states which must reflect the state of the system. Note that the transition graphs are nested to reduce complexity; the lower-level graphs capture substate information.

In the Gate substate of the Cycling state, for example, each channel develops its view of system status based on control state information for each of the four channels. This kind of consensus is one of the major determinants in calculating the operational state of the system. In all, the implementation of this design necessitates a substantial expansion of the logic in the flight code. First, however, it is necessary to examine the system-level coordination logic in terms of meeting the timing constraints given in table 4.5-1.

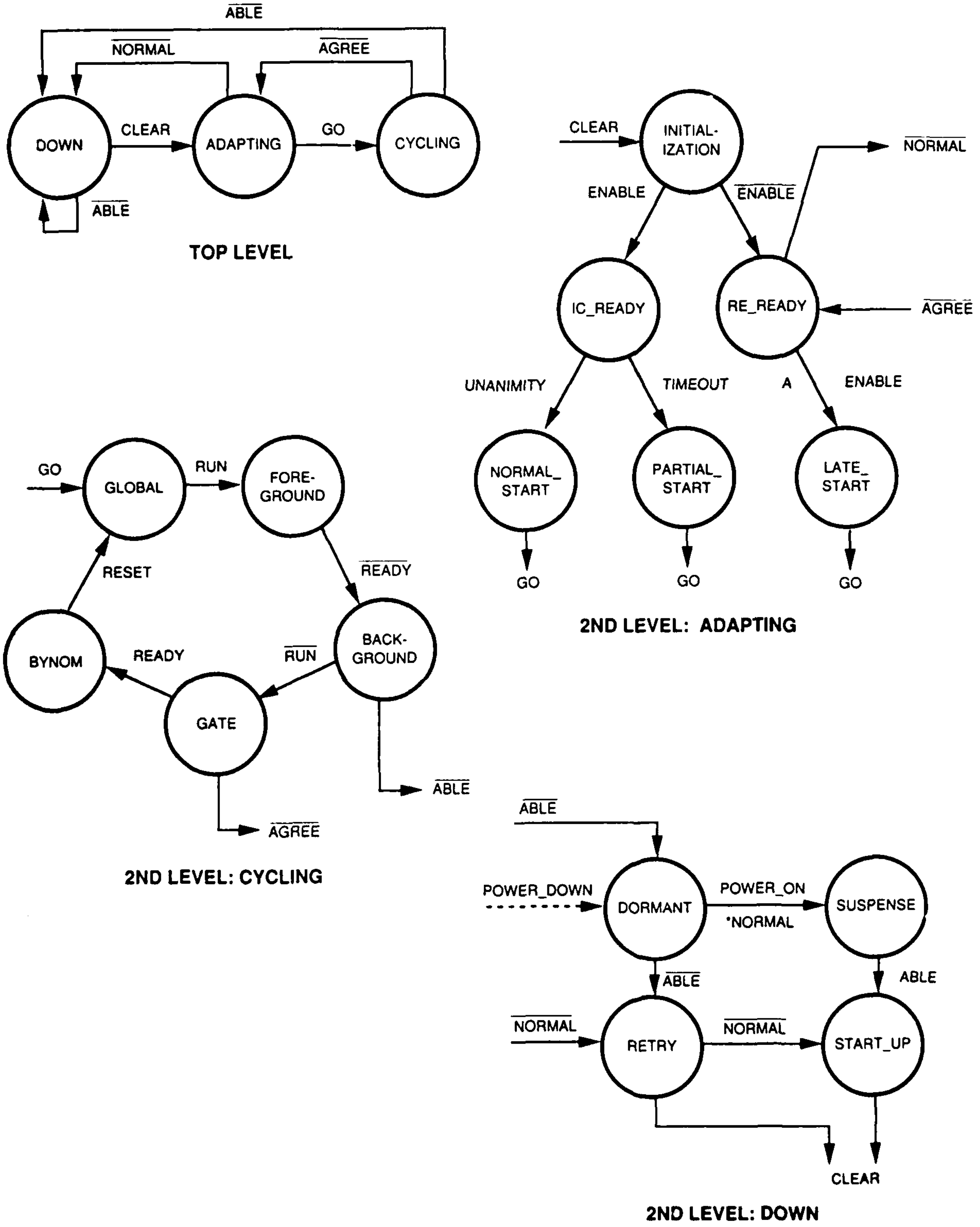


FIGURE 4.5-1. TOP-LEVEL DIGITAL FLIGHT CONTROL SYSTEM CHANNEL LOGIC DESIGN

TABLE 4.5-1. CYCLING STATE LOOP TIMING

| EVENT | Substate and Duration | | | | |
|---|---|---|---|---|---|
| | Global (0-1 msec) | Foreground (1-tfg) | Background (tfg-48) | Gate (48-49) | Synch (49-50) |
| Run | False | True | True | False | False |
| Ready | True | True | False | False | True |
| Reset | True | False | False | False | False |

NOTES: Computational frame time = 50 msec; tfg <48 msec (where tfg is foreground time); timer interrupt at t = 48 msec ≥run; reset ≥t = 0.

System synchronization logic with a discrete time-base imposed is shown in figure 4.5-2, which represents a predicate/transition network (Goldberg, 1979). This view represents only one channel, but all four channels are the same for the subject architecture. Here the same logic nomenclature is retained where applicable, and some new logic variables are added. The logic names appear in the rounded boxes, which are called places in the network. At any given time, the collective values of all the places constitute the state of the system modeled. To examine and verify the correctness of all possible state sequences, the network's operation must be simulated using a computer program. Properly accomplished, such a simulation, under both faulted and fault-free conditions, verifies the system logic design.

The simulation is based on the firing of transitions (denoted by the rectangles in figure 4.5-2), which yield new values for the logic variables stored in the places. The top half of each transition box designates a predicate whose satisfaction by system logic values enables it to be fired. Whenever a transition fires, the new logic values described in the bottom half of the rectangle are assigned. These values are then reflected in the appropriate places, and a new network state produces a new set of transitions that can be fired.

This mechanism can be seen more clearly by noting the partial network in figure 4.5-3. Here the network captures a design where the hardware initialization within a channel sets its POWER ON to TRUE and its CLEAR to FALSE. This arms the top transition, whose firing corresponds to software initialization that sets CLEAR to TRUE among other logic-variable assignments shown. Referring to figure 4.5-3, note that the event of CLEAR being set to TRUE effects the top-level channel state transition from DOWN to ADAPTING. At this point, the channel tries to synchronize with the other channels, to enter the CYCLING state.

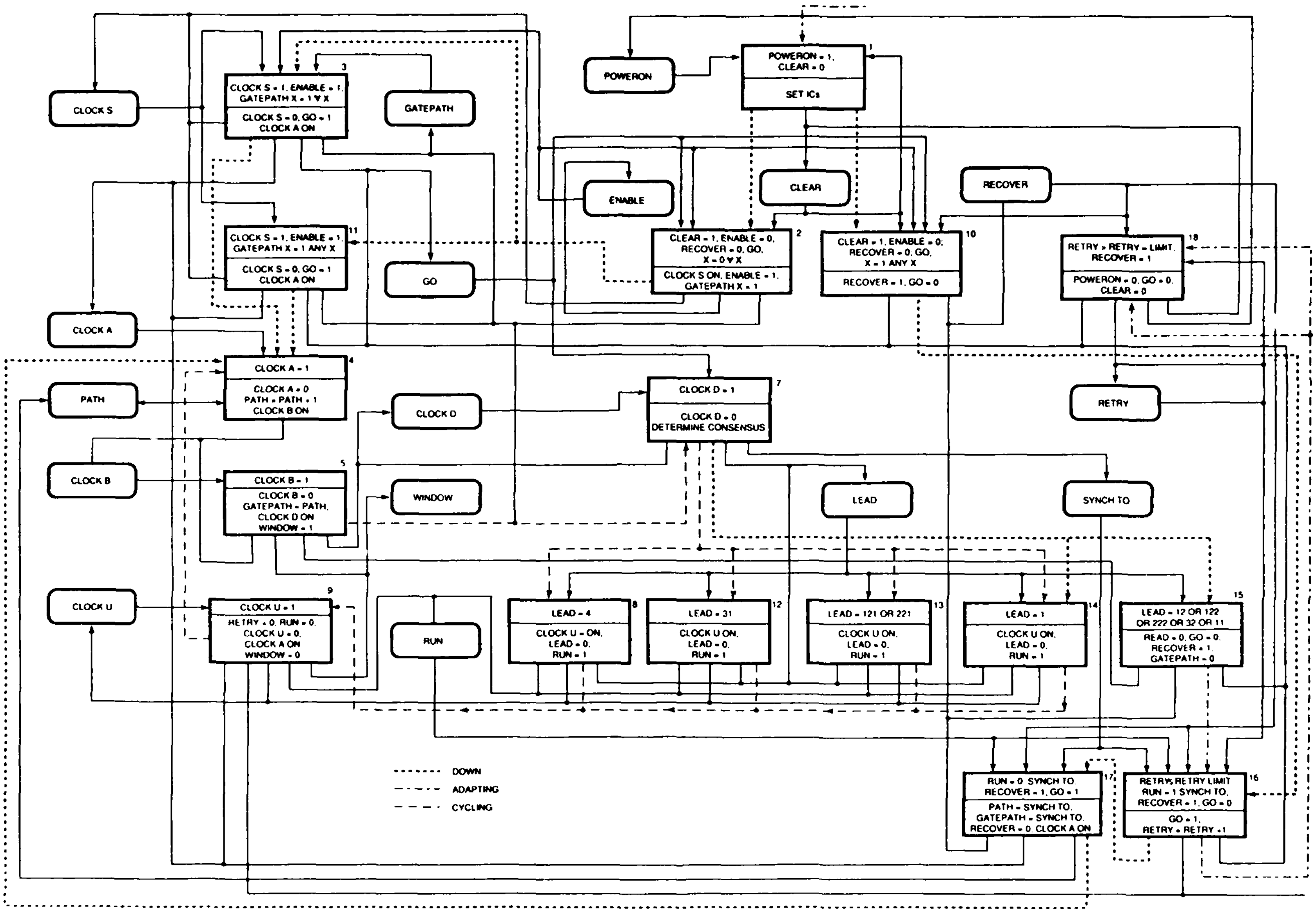

CLOCK S
CLOCK S = 1, ENABLE = 1, GATEPATH X = 1 ∀ X
CLOCK S = 0, GO = 1 CLOCK A ON
3
GATEPATH
POWERON
POWERON = 1, CLEAR = 0
SET ICs
1
ENABLE
CLEAR
RECOVER
CLOCK S = 1, ENABLE = 1, GATEPATH X = 1 ANY X
CLOCK S = 0, GO = 1 CLOCK A ON
11
GO
CLEAR = 1, ENABLE = 0, RECOVER = 0, GO, X = 0 ∀ X
CLOCK S ON, ENABLE = 1, GATEPATH X = 1
2
CLEAR = 1, ENABLE = 0; RECOVER = 0, GO, X = 1 ANY X
RECOVER = 1, GO = 0
10
RETRY > RETRY - LIMIT, RECOVER = 1
POWERON = 0, GO = 0, CLEAR = 0
18
CLOCK A
CLOCK A = 1
CLOCK A = 0 PATH = PATH + 1 CLOCK B ON
4
PATH
CLOCK D
CLOCK D = 1
CLOCK D = 0 DETERMINE CONSENSUS
7
RETRY
CLOCK B
CLOCK B = 1
CLOCK B = 0 GATEPATH = PATH, CLOCK D ON WINDOW = 1
5
WINDOW
LEAD
SYNCH TO
CLOCK U
CLOCK U = 1
RETRY = 0, RUN = 0, CLOCK U = 0, CLOCK A ON WINDOW = 0
9
RUN
LEAD = 4
CLOCK U = ON, LEAD = 0, RUN = 1
8
LEAD = 31
CLOCK U ON, LEAD = 0, RUN = 1
12
LEAD = 121 OR 221
CLOCK U ON, LEAD = 0, RUN = 1
13
LEAD = 1
CLOCK U ON, LEAD = 0, RUN = 1
14
LEAD = 12 OR 122 OR 222 OR 32 OR 11
READ = 0, GO = 0, RECOVER = 1, GATEPATH = 0
15
DOWN
ADAPTING
CYCLING
RUN = 0 SYNCH TO, RECOVER = 1, GO = 1
PATH = SYNCH TO, GATEPATH = SYNCH TO, RECOVER = 0, CLOCK A ON
17
RETRY≤RETRY LIMIT RUN = 1 SYNCH TO, RECOVER = 1, GO = 0
GO = 1, RETRY = RETRY +1
16

FIGURE 4.5-2. SYNCHRONIZATION PREDICATE/TRANSITION NETWORK

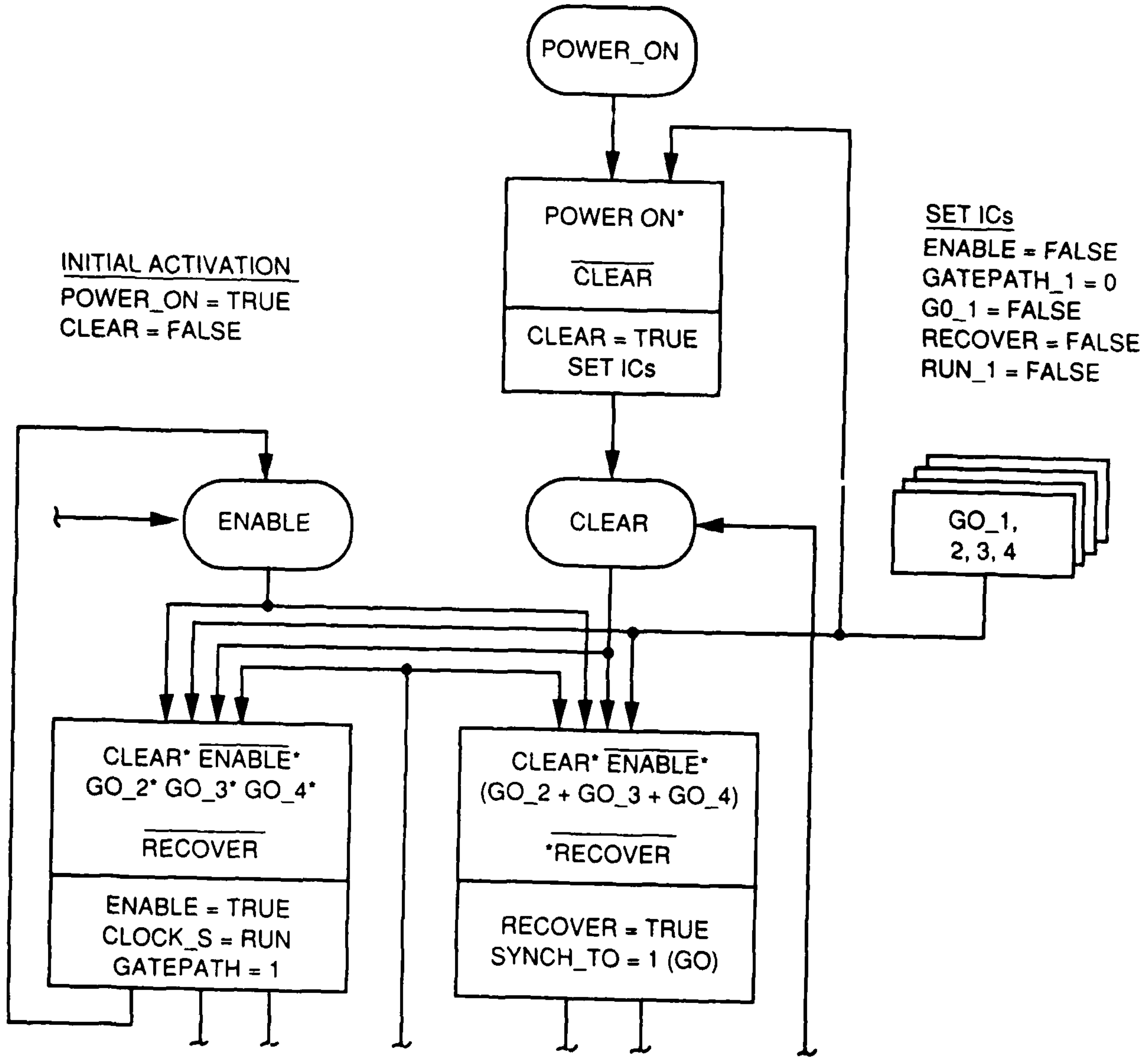


FIGURE 4.5-3. PARTIAL PREDICATE/TRANSITION NETWORK

Network simulation should always yield acceptable system states, and should never terminate unless all channels are failed. Determining that this is the case is a matter of defining and obtaining correct logic operation. In the demonstration, this was accomplished (with one exception noted later). Figure 4.5-4 illustrates some typical discrete-event simulation results for four-way channel synchronization. The pulses at the top indicate instances where individual channels were forced out of synchronization; that is, the corresponding logic-variable RECOVER went TRUE. The resynchronization logic in the network model then satisfactorily restored synchronization, and the RECOVER was set to FALSE, as indicated by the end of the pulse in figure 4.5-4.

Following synchronization design verification, which captured time-based hardware/software interaction, the design emphasis shifted to the top-level software design with the constraints imposed by the existing RDFCS hardware.

In the basic system, the flight software is hardware-interrupt-driven at the 60-Hz rate. Since the AFBW control laws were designed for 20-Hz operation, the executive software invokes the applications control functions every third interrupt. The executive program itself is somewhat austere, as appropriate for a dedicated system. Here the computational channels mutually coordinate themselves in a frame-synchronous, double fail-operational manner.

To achieve this, the channel design must be mapped into a software design with the objectives of maintaining consistency in the system-to-software design transition and minimizing the complexity of the software. Accordingly, the control graph shown in figure 4.5-5 represents a mapping of the top-level transition graph in figure 4.5-1 to a software control structure that preserves the design logic in a form exhibiting only moderate decision-logic complexity as measured by the cyclomatic complexity number. (This number is a measure of program complexity, thus a measure of program testability, maintainability, and, by implication, reliability. The number is a function of the number of control graph vertices, edges, and connected components. See McCabe, 1976 for details.) As byproducts, the control graph yielded test-case input vectors and logic assertions that were later used in verifying the implemented code.

## 4.6. Establishing System Reliability

To establish system reliability and the required architecture, a tradeoff study must be conducted. In establishing system reliability, the reliability assessments are directed toward contrasting levels and types of redundancy relative to their effect on system reliability for critical functions. Table 4.6-1 delineates 12 different system architectures for critical system function failure on both 5- and 10-hour missions. The system architecture shown in figure 2-1 actually corresponds to cases 1 and 2 in table 4.6-1, depending on whether inherent backup capability is invocable. Because of the arrangement of the mode-selection switch that was devised in the RDFCS laboratory, the backup mode was manually selectable. Figure 4.6-1 represents the reliability model for architecture case 1, the one actually implemented. Note that the dependencies and logic embedded in this reliability model do not, however, apply to case 2 in table 4.6-1.

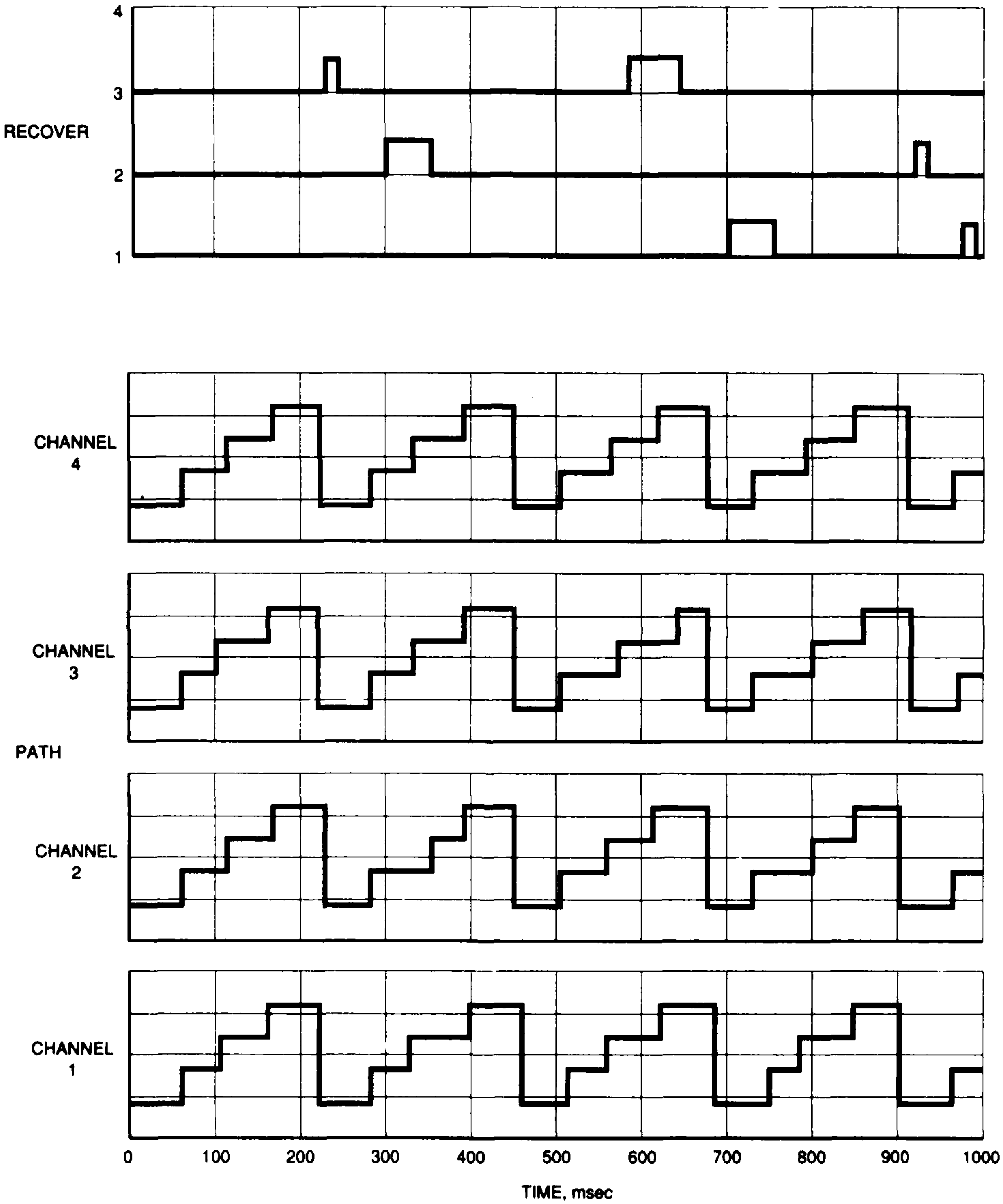


FIGURE 4.5-4. TYPICAL DISCRETE-EVENT SIMULATION RESULTS

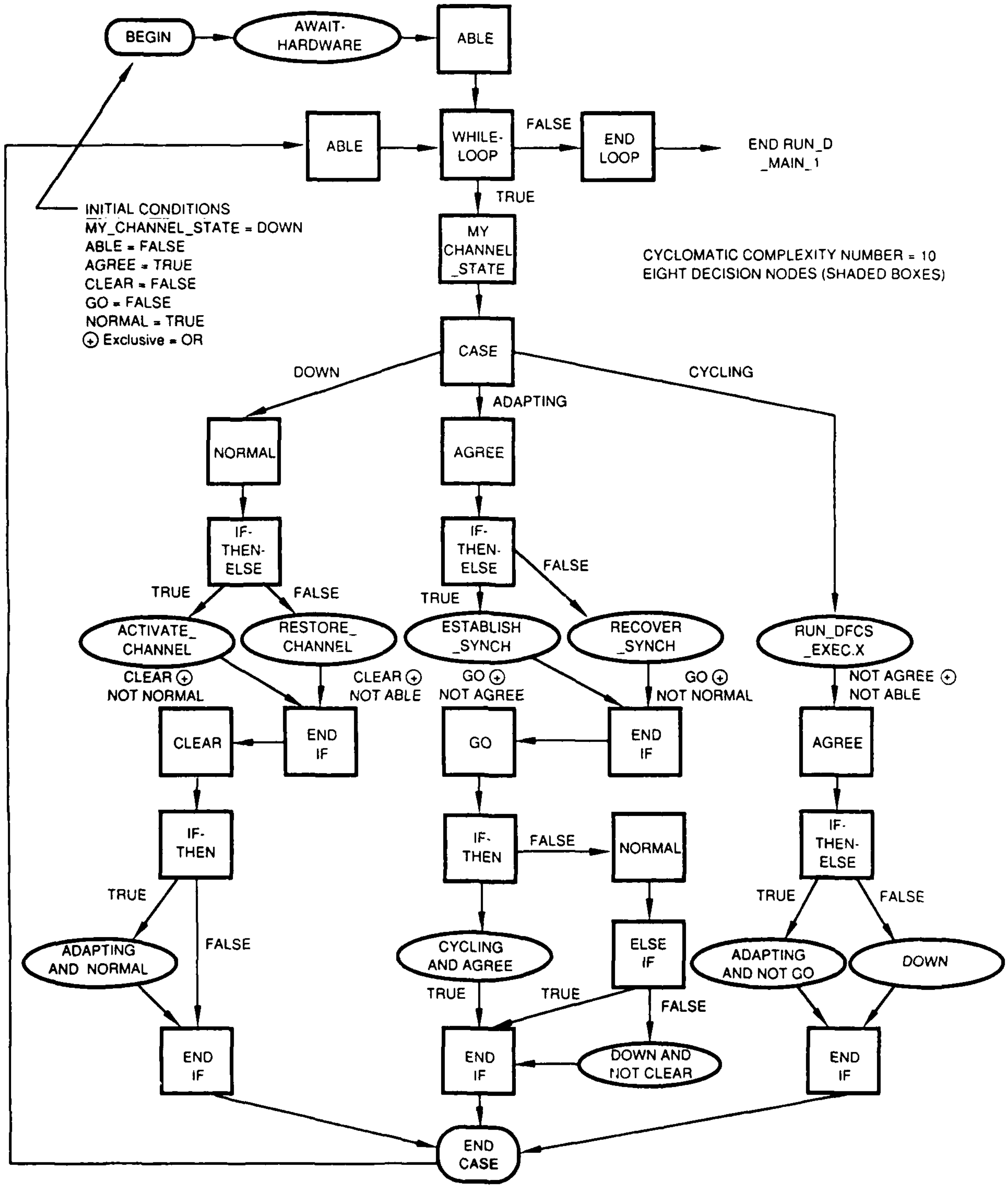
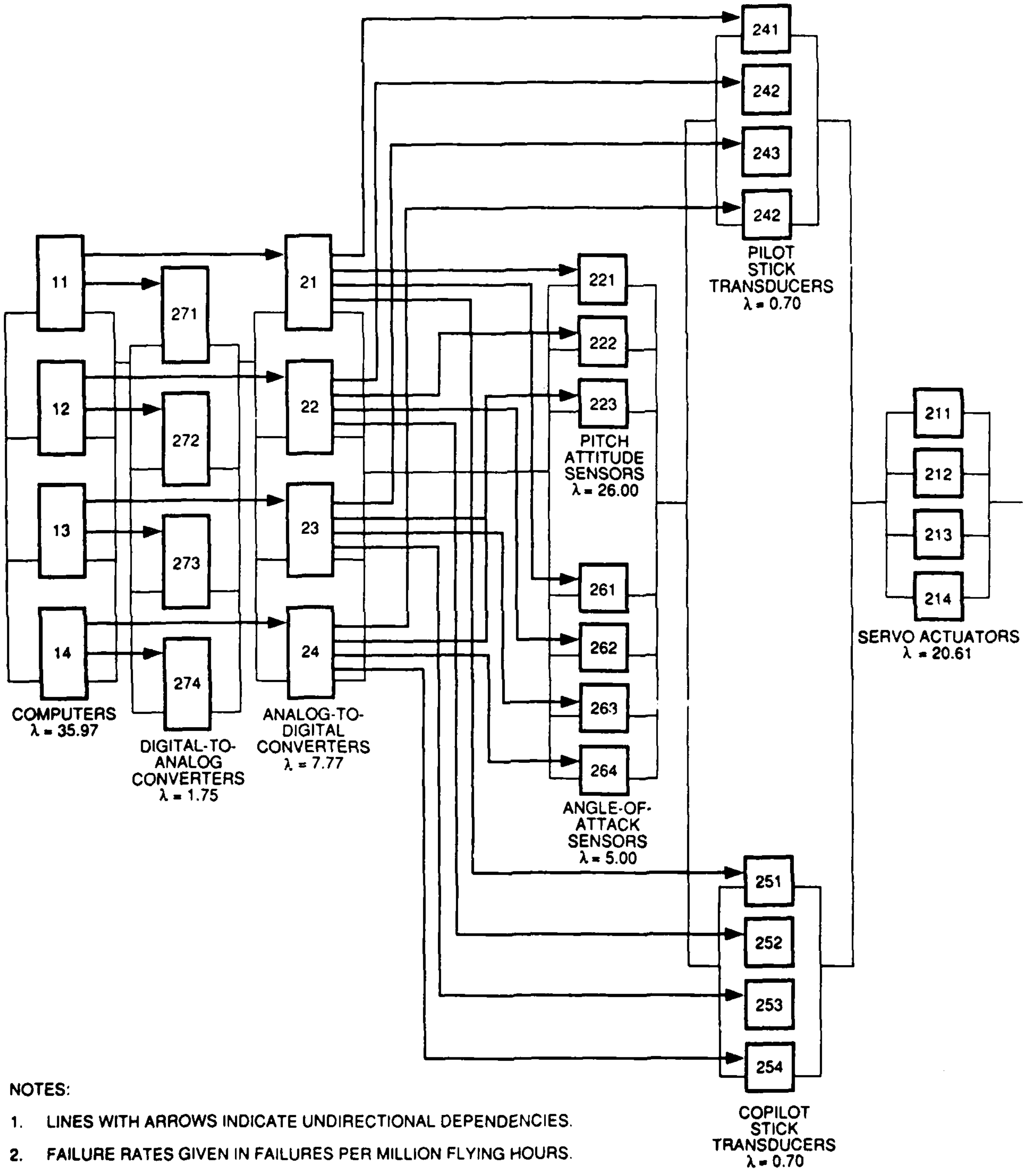


FIGURE 4.5-5. CONTROL GRAPH OF TOP-LEVEL SOFTWARE



241
242
243
242
PILOT STICK TRANSDUCERS λ = 0.70
11
12
13
14
COMPUTERS λ = 35.97
271
272
273
274
DIGITAL-TO-ANALOG CONVERTERS λ = 1.75
21
22
23
24
ANALOG-TO-DIGITAL CONVERTERS λ = 7.77
221
222
223
PITCH ATTITUDE SENSORS λ = 26.00
261
262
263
264
ANGLE-OF-ATTACK SENSORS λ = 5.00
211
212
213
214
SERVO ACTUATORS λ = 20.61
251
252
253
254
COPILOT STICK TRANSDUCERS λ = 0.70

NOTES:

1. LINES WITH ARROWS INDICATE UNDIRECTIONAL DEPENDENCIES.
2. FAILURE RATES GIVEN IN FAILURES PER MILLION FLYING HOURS.
3. BUS AND CONNECTOR FAILURES INCLUDED.

FIGURE 4.6-1. RELIABILITY MODEL FOR IMPLEMENTED ARCHITECTURE

TABLE 4.6-1. DIGITAL FLIGHT-CONTROL SYSTEM RELIABILITY ASSESSMENTS

| Case | System | SAS Backup | Servo Setup | Failure Probability | |
|---|---|---|---|---|---|
| | | | | 5 hour | 10 hour |
| 1 | Quad AFBW | Pitch hold | Quad | $0.478X10^{-10}$ | $0.382X10^{-9}$ |
| 2 | Quad AFBW | None | Quad | $0.615X10^{-10}$ | $0.492X10^{-9}$ |
| 3 | Quad AFBW | None | Triplex | $0.626X10^{-10}$ | $0.500X10^{-9}$ |
| 4 | Quad AFBW | None | Dual-dual | $0.107X10^{-7}$ | $0.430X10^{-7}$ |
| 5 | Dual-dual AFBW | None | Dual-dual | $0.200X10^{-6}$ | $0.798X10^{-6}$ |
| 6 | Quad FBW | N/A | Quad | $0.457X10^{-10}$ | $0.365X10^{-9}$ |
| 7 | Quad FBW | N/A | Triplex | $0.468X10^{-10}$ | $0.374X10^{-9}$ |
| 8 | Triplex FBW | N/A | Triplex | $0.153X10^{-6}$ | $0.612X10^{-6}$ |
| 9 | Quad SAS | Pitch hold | Quad | $0.478X10^{-10}$ | $0.382X10^{-9}$ |
| 10 | Quad SAS | None | Quad | $0.615X10^{-10}$ | $0.491X10^{-9}$ |
| 11 | Quad SAS | None | Triplex | $0.626X10^{-10}$ | $0.500X10^{-9}$ |
| 12 | Triplex SAS | None | Triplex | $0.188X10^{-6}$ | $0.751X10^{-6}$ |

The cases of primary interest here (1 through 5 in table 4.6-1) are all-up AFBW architectures. Cases 1 through 3 meet the critical-function reliability requirements defined in Defeo, Doane, and Saito, 1982, but the analyses only take into account the hardware fault contributions to unreliability. Still, the data are instructive in several ways. Basically, the backup pitch-hold mode adds surprisingly little to survivability, partly because it would be needed so infrequently, and then only at a time when it too might well be unavailable owing to the loss of common components with the basic pitch Stability Augmentation System (SAS).

Cases 4 and 5 (table 4.6-1) are inadequate because of reduced redundancy levels. Cases 5 through 7 isolate the reliability properties of straight FBW architectures. A comparison of cases 2 and 6 shows, for example, that the critical pitch SAS function increases the probability of failure by about only a third for a straight FBW system. The straight SAS function is isolated in cases 9 through 12, and it is noteworthy that triplex AOA sensors and computers are inadequate for case 12. However, triplex servos with quadruplex sensors are satisfactory.

Tables 4.6-2 and 4.6-3 reveal flying-qualities degradation, as well as system failure, the extent and likelihood of the degradation being important measures of system acceptability. Cases 6 through 8 are omitted because the straight FBW function does not degrade in stages; instead, it usually fails completely when an appropriate combination of failures has occurred. Since stability-augmentation degradation is basically sensor-related, this set of servo-oriented architecture variations is not fully useful in delineating flying-qualities tradeoffs.

TABLE 4.6-2. DEGRADATION OF FLYING-QUALITIES: 5-HOUR MISSION

| Case* | Flying-Qualities Level (probability) | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | <3 |
| 1 | 0.999+ | 0.212X10$^{-6}$ | 0.017X10$^{-11}$ | 0.478X10$^{-10}$ |
| 2 | 0.999+ | 0.212X10$^{-6}$ | 0 | 0.615X10$^{-10}$ |
| 3 | 0.999+ | 0.212X10$^{-6}$ | 0 | 0.626X10$^{-10}$ |
| 4 | 0.999+ | 0.212X10$^{-6}$ | 0 | 0.607X10$^{-10}$ |
| 5 | 0.999+ | 0.120X10$^{-3}$ | 0 | 0.200X10$^{-6}$ |
| 9 | 0.999+ | 0.212X10$^{-6}$ | 0.137X10$^{-10}$ | 0.478X10$^{-10}$ |
| 10 | 0.999+ | 0.212X10$^{-3}$ | 0 | 0.615X10$^{-10}$ |
| 11 | 0.999+ | 0.212X10$^{-6}$ | 0 | 0.626X10$^{-10}$ |
| 12 | 0.999+ | 0.221X10$^{-6}$ | 0 | 0.188X10$^{-6}$ |

*Cases 6 through 8 omitted because the FBW function does not degrade in stages (it fails completely given appropriate combinations of failures).

TABLE 4.6-3. DEGRADATION OF FLYING-QUALITIES: 10-HOUR MISSION

| Case* | Flying-Qualities Level (probability) | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | <3 |
| 1 | 0.999+ | 0.848X10$^{-6}$ | 0.250X10$^{-14}$ | 0.382X10$^{-9}$ |
| 2 | 0.999+ | 0.848X10$^{-6}$ | 0 | 0.492X10$^{-9}$ |
| 3 | 0.999+ | 0.848X10$^{-6}$ | 0 | 0.500X10$^{-9}$ |
| 4 | 0.999+ | 0.848X10$^{-6}$ | 0 | 0.430X10$^{-7}$ |
| 5 | 0.999+ | 0.240X10$^{-3}$ | 0 | 0.798X10$^{-6}$ |
| 9 | 0.999+ | 0.819X10$^{-6}$ | 0.108X10$^{-9}$ | 0.382X10$^{-9}$ |
| 10 | 0.999+ | 0.848X10$^{-6}$ | 0 | 0.492X10$^{-9}$ |
| 11 | 0.999+ | 0.848X10$^{-6}$ | 0 | 0.500X10$^{-9}$ |
| 12 | 0.999+ | 0.883X10$^{-6}$ | 0 | 0.751X10$^{-6}$ |

*Cases 6 through 8 omitted because the FBW function does not degrade in stages (it fails completely given appropriate combinations of failures).

However, certain factors are of interest. Cases 11 and 12, although they show only a slight increase in flying-qualities degradation for the fully triplex architecture, indicate a notable disposition toward system failure. This suggests that the triplex computers are a weaker point in configuration 12 than are the three AOA pairs. Case 8 (table 4.6-1) tends to reinforce this inference.

The architectures used here are based on earlier-design DFCSs that have been used in retrofitting aircraft that had previously used analog systems. In retrofitted systems the interconnecting wiring is usually dedicated point-to-point signal paths, with little use of Multiplexer (MUX) busses. Newer systems commonly use parallel MUX buses, and considerably more complex bus topologies will be used when true digital computational capability comes into common use. Newer systems will use broader bandwidths, damage tolerance, and soft-fault processing. As a result, extended Mean Time Between Failures (MTBF) of up to 90,000 hours and system availabilities of 0.95 at a service life of 40,000 hours will be achieved. Considerably more system integration will also lead to additional diversity in MUX bus organization.

## 4.7. The Airplane Simulation

A negative static stability margin was postulated as a requirement for this demonstration, and six RSS flight cases were developed. These flight cases are then analyzed to determine the pitch-axis dynamic behavior, and a non-real-time simulation is developed and checked against the predicted pitch-axis dynamics for the free or, unaugmented, airplane. The same flight-case data are then used in the RDFCS facility simulation. Next, the non-real-time simulation time-history responses are used to check the RDFCS simulation.

Both the non-real-time and the RDFCS simulations discussed in this chapter are implemented using a state-variable approach (figure 4.7-1). Here the pitch-axis dynamics of the free RSS airplane, as captured in the matrix A (figure 4.7-1), are quite divergent or unstable, so certain states must be fed back to enable a stability augmentation function. The state variables here are pitch, pitch rate, vertical-axis velocity, and horizontal-axis velocity. The first two states are inertially oriented and are directly measured by airplane sensors. The second two are referenced to the airstream incident on the airplane, and are combined to form the directly measured signals: AOA and true airspeed. These two air-data signals are produced using matrix C.

The above sensor feedback signals then appear in vector u (figure 4.7-1). Pilot stick inputs are applied through vector d.

Table 4.7-1 summarizes conversions of six basic wide-body transport-type flight cases to six corresponding RSS flight cases with -5 percent static stability margins. For flight case A1RSS, for example, calculations revealed the neutral point to be 53 percent of the Mean Aerodynamic Chord (MAC), where neutrality denotes that there is no pitch-moment change with change in AOA. More specifically, the stability derivative describing the airframe behavior goes to zero. The -5 percent static margin then corresponds to shifting the center of gravity aft to 58 percent MAC.

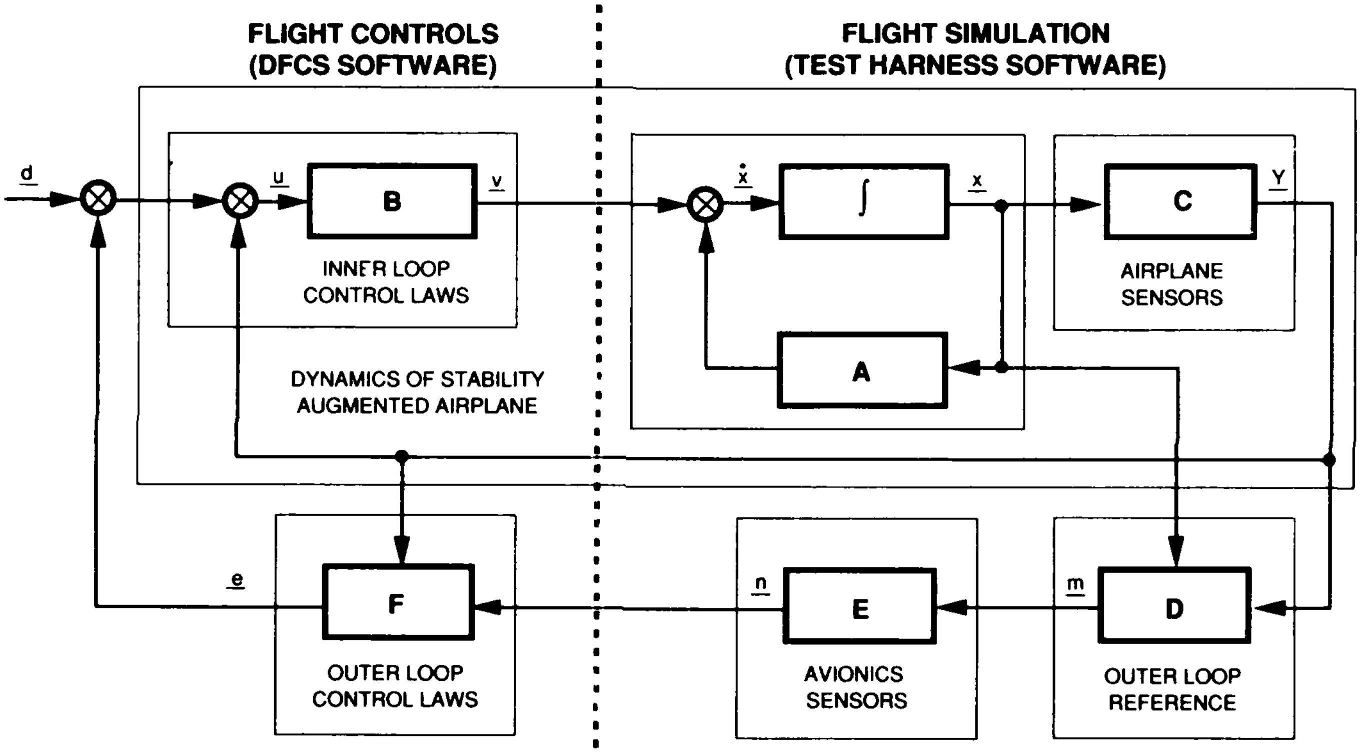


FIGURE 4.7-1. DIAGRAM OF STATE-VARIABLE AIRPLANE SIMULATION

TABLE 4.7-1. RELAXED STATIC STABILITY FLIGHT CASES

| Parameter | A1RSS | C13RSS | C15RSS | D2RSS | F3RSS | F6RSS |
|---|---|---|---|---|---|---|
| c.g., %$\bar{c}$ | 58.0 | 51.0 | 54.2 | 52.8 | 55.5 | 64.4 |
| Neutral point, %$\bar{c}$ | 53.0 | 46.0 | 49.2 | 47.8 | 47.8 | 49.4 |
| $V_T$, ft/sec | 283.7 | 910.7 | 442.2 | 487.1 | 265.7 | 224.1 |
| $\tau_1$, sec | 1.099 | 0.160 | 0.122 | 0.660 | 0.938 | 0.920 |
| $\tau_2$, sec | -5.86 | -2.40 | -1.64 | -7.55 | -7.09 | -3.17 |
| $\omega_{PH}$, rad/sec | 0.169 | 0.008 | 0.134 | 0.125 | 0.167 | 0.209 |
| $\zeta_{PH}$ | 0.276 | 0.325 | 0.526 | 0.453 | 0.488 | 0.192 |
| $\Delta C_M/\Delta\delta_H$, 1/rad | -3.247 | -2.830 | -2.415 | -2.533 | -3.138 | -3.016 |
| $\Delta C_M/\Delta_q$, 1/rad | -11.48 | -14.99 | -12.15 | -12.75 | -11.76 | -11.23 |
| $\Delta C_M/\Delta$ , sec/rad | -3.14 | -7.83 | -3.44 | -3.18 | -3.14 | -3.03 |
| $\Delta C_M/\Delta C_L$ | 0.050 | 0.044 | 0.053 | 0.050 | 0.053 | 0.170 |
| $\Delta C_M/\Delta$ , 1/rad | 0.295 | 0.353 | 0.288 | 0.292 | 0.306 | 0.960 |

This kind of alteration to the airframe dynamics yields a pair of real or non-oscillatory roots, $\tau_1$ and $\tau_2$ in table 4.7-1. Note that the negative time-constants for $\tau_2$ correspond to positive roots, which plot on the positive axis of the s-plane and produce an absolute instability or exponential divergence that dominates the dynamic response of the airplane's pitch axis. With a -5 percent margin, moreover, the rate of divergence is quite rapid and clearly unacceptable. For flight case F6RSS, for example, the 3.17 second time-constant yields a doubling of pitch attitude in 2.2 seconds, which is so rapid as to be unflyable.

A non-real-time simulation was used to generate airplane time-history check cases before work was begun at the RDFCS simulator. The organization of the previously been installed in the simulator test computer. For the RSS flight cases, no changes were made to the software organization itself, other than to add interfaces for the SAS control laws. The organization of the simulation provides for the conversion of flight-case data into a discrete-time model, trimming for specified initial conditions, and generation of dynamic time-history outputs. Ground effects, random gust options, or point simulation flight-case transitions may be selected.

Two stages of analysis were performed. First, the RSS airplane behavior was approximated by shifting the center of gravity aft to -5 percent MAC. It should be noted that six of the old flight cases have been converted into six derivatives sensitive to the reduced lever-arm of the empennage about the new center of gravity. As indicated in table 4.7-1, these all relate to the generation of a pitching moment. The analyses of the RSS flight cases then involved the examination of their respective dynamics. Specifically, the RSS stability derivatives were used to calculate the free-airplane response by finding the root solutions to the characteristic equation for each flight case. These results are also given in table 4.7-1.

Note that the sign on the pitching moment, owing to wing-lift, changes from negative for 25 percent to positive for 58 percent MAC. In the RSS case then, increasing lift produces more nose-up moment, which in turn further increases lift. This positive feedback causes an instability in the free, or unaugmented, airplane response. The rate of divergence is quite rapid. For flight case F6RSS, for example, the time-constant of -3.17 seconds yields a doubling of pitch attitude every 2.2 seconds. The given time-constants, radial frequencies, and damping ratios were obtained from the root solutions of the characteristic equations for the respective flight cases, as determined by the stability derivatives.

Simulation check cases were first run using the non-real-time dynamic simulation. Time-histories were generated for each case and checked against the root solutions. For the RSS cases, the divergent real root dominated the time-histories. The pitch-angle sequence exhibits an exponential time-constant roughly the same as the analytical calculated time-constant value of -3.17 seconds for flight case F6RSS once the initial transient has subsided. The initial upset of 3.0 degrees per second of pitch rate employed here is not really needed to exhibit the instability. It is used as a standard upset as needed for the corresponding augmented airplane.

Whereas these free-airplane responses are used as a cross-check on the real-time airplane simulation, the augmented airplane response is used to check both the simulation and the stability-augmentation control laws. Analytical-root-solution (eigenvalue) checks can also be made for the augmented airplane response, where the order of the characteristic equations is increased as a result of the presence of the sensor feedbacks. All these checks should be in general agreement. They then serve to corroborate the control laws used in different stages of development.

In general, the requirement for stability augmentation is to effect desirable flying qualities for the augmented airplane. Basically, the eigenvalues of the closed-loop airplane should exhibit suitable damping and frequency characterisclosed-loop airplane should exhibit suitable damping and frequency characteristics. In effect, the augmentation control law should override the RSS airplane's positive pitching moment caused by increasing wing lift. Restoration of the negative pitching moment is possible through a nose-down stabilizer input for increasing AOA.

For the subject demonstration, the design criterion was simply to provide approximately the same, or better, pitch-axis handling and response for the stability-augmented RSS airplane than was available on the basic 25 percent MAC center-of-gravity free airplane.

## 5. VERIFYING THE SIMULATION

There are two major concerns with the verification of DFCSs: cross-channel synchronization and cross-channel consensus. Cross-channel synchronization poses the greater challenge because coincident, wideband access to the required logic signals, either hardware or software, usually demands some special instrumentation. In addition, means must be provided for rapidly appraising the observed logic states so that anomalies can be noted and captured before new events mask the attendant circumstances. Such appraisals must correlate events over the different channels, as well as reference external events such as fault insertions. For closure on assurance objectives, the online assessment must be based on precise representations of the verified design. These then constitute real-time test criteria when incorporated into execution monitors.

Observation and assessment of system availability and function/mode states are more tractable because of relaxed bandwidth requirements. Moreover, monitoring hardware test points is not generally necessary. The overall magnitude and complexity of the associated logic considerations means that a substantial amount of logic must be monitored. It is therefore desirable to minimize the number of logic variables that must be monitored. Perhaps the most formidable problem for the system monitor is that of judiciously defining test cases. The intent here is to maximize system-level coverage while acknowledging the unit-level test cases and coverage of previous programs. This is, of course, an issue largely independent of the construction and operation of the execution monitor itself. Note that in the case of the cross-channel synchronization monitor, previous unit-level testing is not very significant. This is because definitive testing is possible only after the hardware/software is available and operating.

As in most exploratory investigations, the scope of the DFCS test article was purposely limited, even though the quadruplex system architecture logic was fully implemented. Appropriate aspects of this logic are examined by two real-time execution monitors. The channel synchronization monitor for this implementation resides in one of the flight computers, and the system state monitor has been installed in the main simulation/test computer. The first monitor examined certain low-level events. On a larger scale it noted the readiness of each channel to operate with the flight-computer consensus.

Here the term consensus refers to the computer subsystem operational state as manifested by the majority of operable computers in terms of their synchronized, cooperative behavior. Most of the flight-computer faults that can occur compromise the affected computer's capacity to function and its ability to participate in this consensus. Such a loss would be noted by the system state monitor directly, as well as in terms of the DFCS system state consensus. Also, the synchronization monitor will capture some of the constituent logic sequences in the respective DFCS channels that culminate in the system state noted.

An automated testing scenario as generalized in figure 5-1 and elaborated on in table 5-1 has been implemented to simulate, observe, and record DFCS coordination phenomena. The test-case design has resulted from analysis of the DFCS specification and design, within the constraints of the capabilities of the test facility. Those constraints discouraged the use of automated test drivers, such as those used in Benson, Mulcare, and Larsen, 1987. However, this is not a significant limitation in this example, in which the emphasis has been on the real-time monitoring and results processing, instead of on testing productivity.

Multilevel testing is used to obtain conclusive evidence of the consistency of the DFCS implementation. Test-case design focuses on the architectural system/software logic indicated in figure 3-2. Here system validation is not at issue, so verification test scripts for the all-up system are devised only for the multiple levels indicated. Actually, these various level test requirements should be by-products of the corresponding stages of system development. The key point is that low-level design and implementation details should be examined simultaneously during system testing.

The DFCS simulator facility was implemented as shown in figure 5-2. The dual-dual architecture was replaced by a double fail-operational (quadruplex) architecture where each channel is relatively independent of all others. As a consequence, only one computer channel would fail at a time. The utility computer is used to retrieve selected software state data, through the test adapters, for the simulation/test computers.

Simulator testing was mechanized as shown in figure 5-3. The system consensus execution monitor, which was in the simulation/test computer, observed each channel's view of the consensus along with certain lower-level logic states. These parallel sets of data were used to check the consistency of the logic states of the operable channels. These states were referenced to the specified system states, according to component availability, and to lower-level logic design descriptions.

Not surprisingly, the bandwidth of the instrumentation computer was inadequate for monitoring and evaluating cross-channel synchronization logic. The fourth DFCS flight computer was used to monitor the synchronization logic of the other three, a function made possible because of the built-in cross-channel serial data transmission broadcast from each channel. This was also the medium used for synchronization control under the software-only modification rules for the test facility. Consequently, the monitor was able to view the synchronization process without having to fetch the wide bandwidth signals of interest.

Table 5-2 provides a breakdown of the multilevel monitoring functions and their focus. All but the fourth category, control flow, have been implemented and run. Still, there was ample quiescent time in the testing part of the system to conduct concurrent additional tests. The purpose of all of the monitors was to observe logic variable changes and their effects on related states. Figure 4 5-1 illustrates state-transition graphs that define the synchronization design within each channel. The monitor can then be interpreted as a data structure for each channel coupled with the specified outcome taken from the system level.

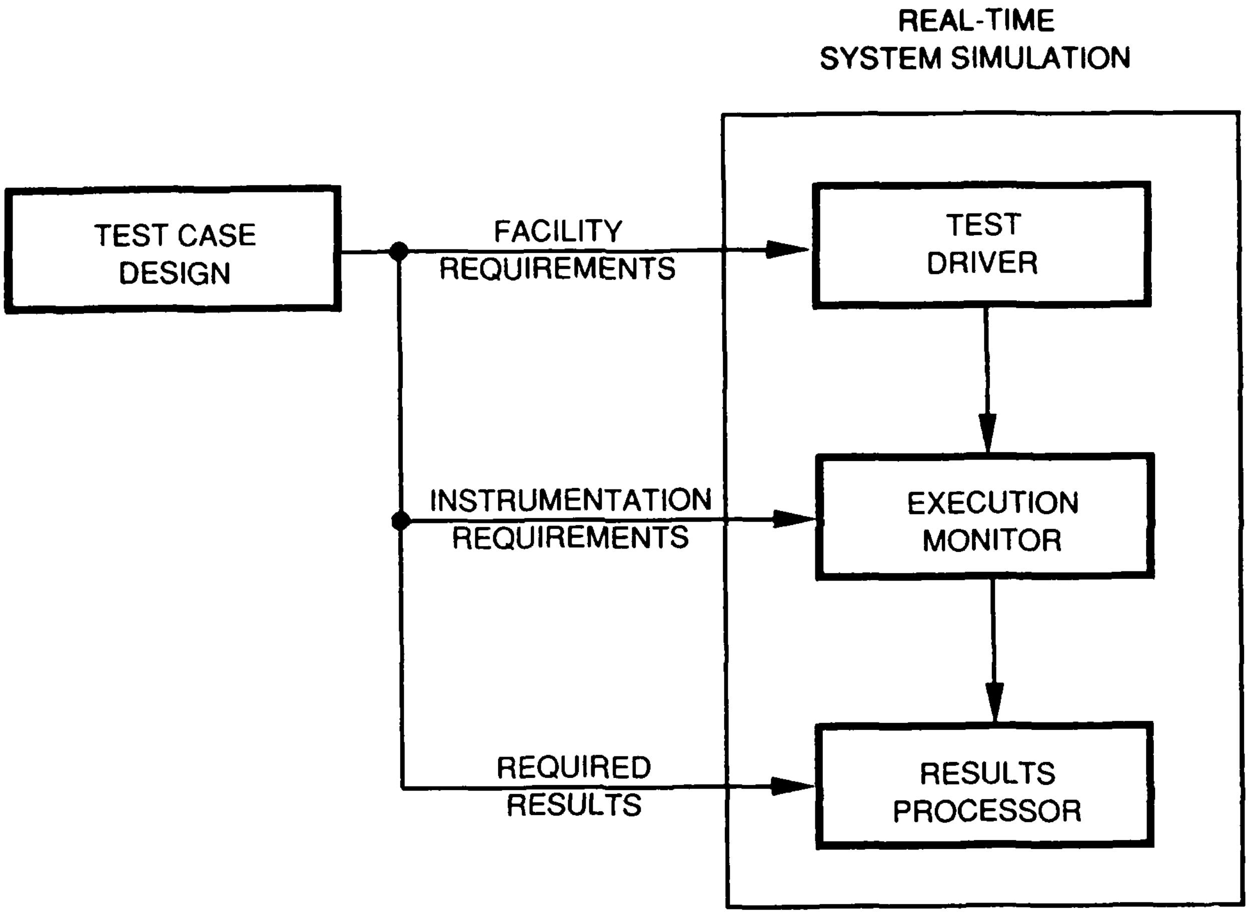


FIGURE 5-1. AUTOMATED TEST SCENARIO

TABLE 5-1. AUTOMATED TESTING TOOLS

| Function | Type of Tool | Purpose |
|---|---|---|
| Test case design | Static analysis | Assessment of properties without actual program execution |
| Test driver | Automated testing | Automated control of test stimuli, environment, and data acquisition in a non-interfering manner |
| Execution monitor | Instrumentation | Implementation of probes for monitoring or recording during program execution |
| Results processor | Dynamic analysis | Assessment of properties during or after program execution |

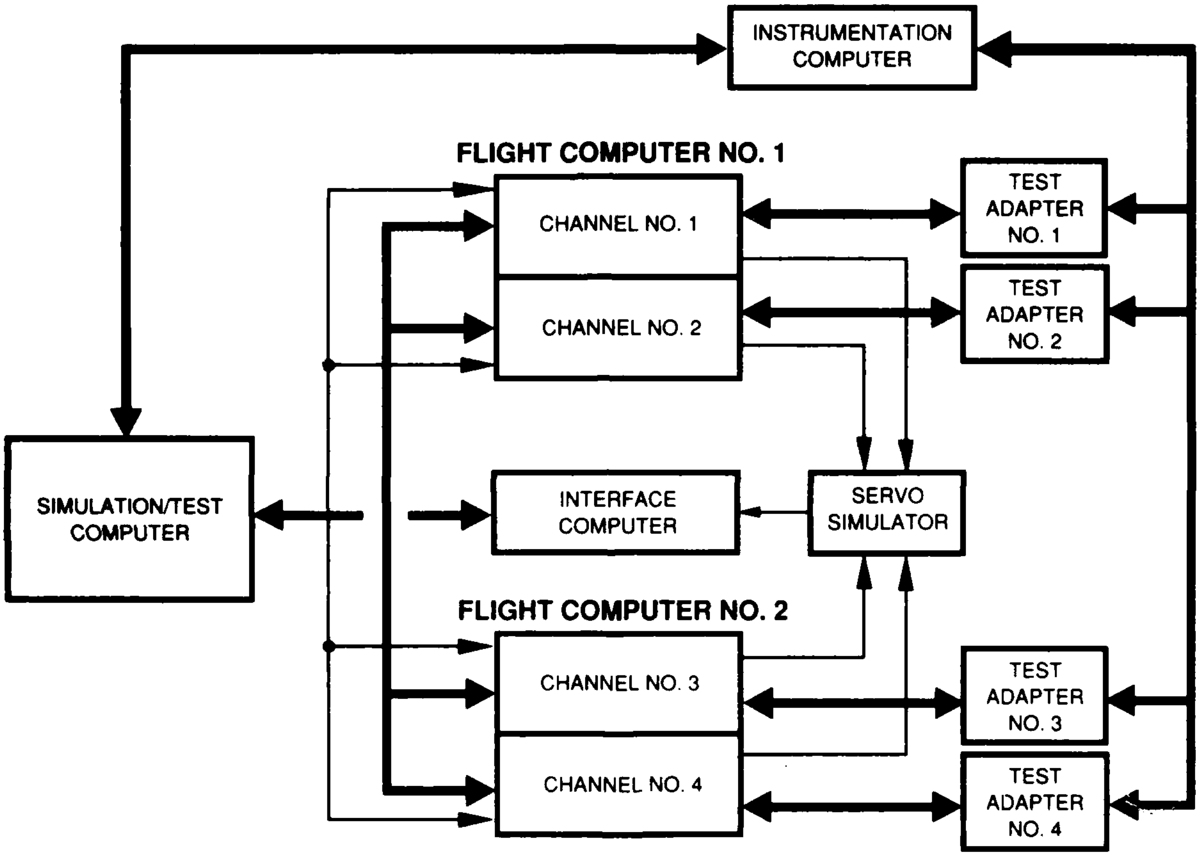


FIGURE 5-2. IMPLEMENTATION OF DIGITAL FLIGHT CONTROL SYSTEM SIMULATOR FACILITY

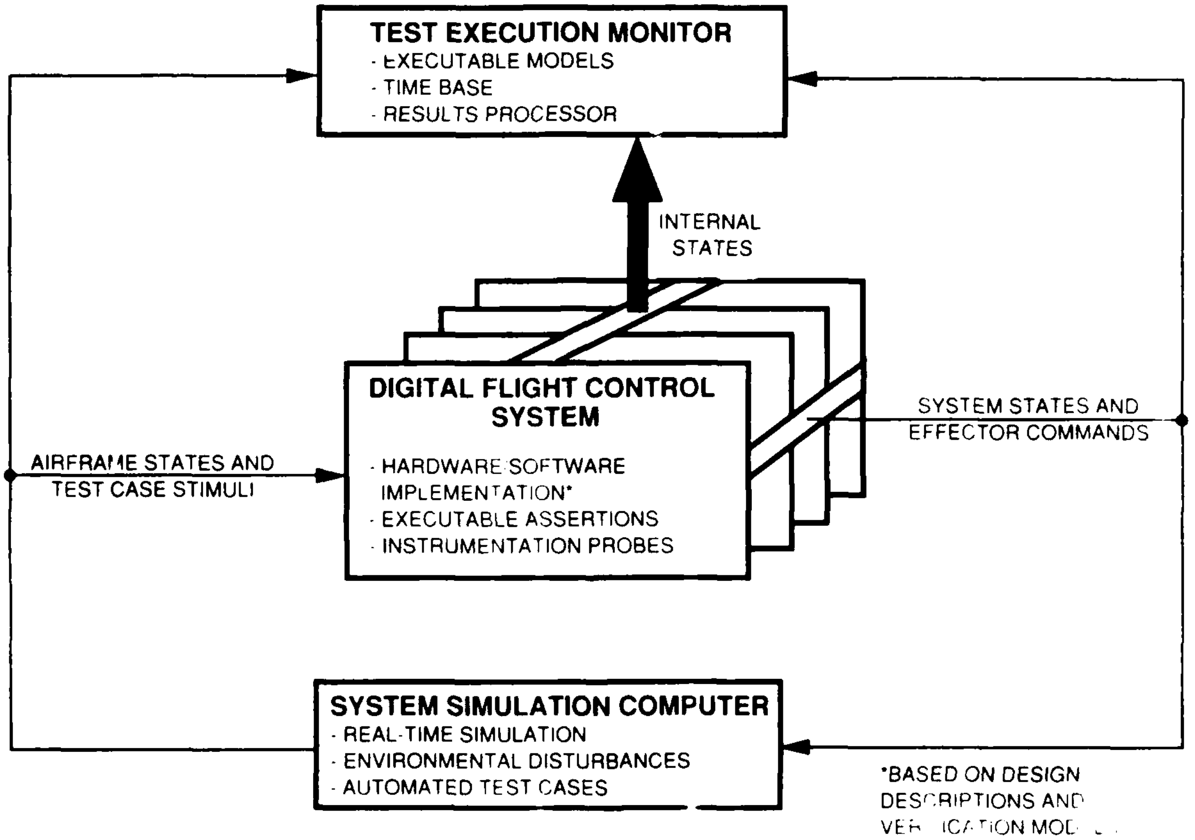

TEST EXECUTION MONITOR
- EXECUTABLE MODELS
- TIME BASE
- RESULTS PROCESSOR
INTERNAL STATES
DIGITAL FLIGHT CONTROL SYSTEM
- HARDWARE/SOFTWARE IMPLEMENTATION*
- EXECUTABLE ASSERTIONS
- INSTRUMENTATION PROBES
AIRFRAME STATES AND TEST CASE STIMULI
SYSTEM STATES AND EFFECTOR COMMANDS
SYSTEM SIMULATION COMPUTER
- REAL-TIME SIMULATION
- ENVIRONMENTAL DISTURBANCES
- AUTOMATED TEST CASES
*BASED ON DESIGN DESCRIPTIONS AND VERIFICATION MODELS

FIGURE 5-3. MECHANIZATION OF SIMULATOR TESTING

TABLE 5-2. MULTILEVEL TEST CASES AND MODES

| Verification Focus | Execution Monitor | Monitor Location | Primary Concern |
|---|---|---|---|
| System State | Nested-state transition graphs | Simulation/test computers | System state consensus |
| Channel synchronization | Nested-state transition graphs | One flight computer channel | Coincidental faults |
| Mode/fault logic | Boolean expressions | Simulator/test computer | Logic correctness |
| Control flow | Control graphs with assertions | One flight computer | Software path traversal |

# 6. SUMMARY

In addition to a variety of simulated hardware fault insertions, the quadruplex DFCS used for this example actually sustained an out-of-tolerance Flight Control Computer (FCC) clock problem during testing. This was at first thought to be a new DFCS design problem, but examination showed that the system was responding properly to discrepant hardware. It is not certain if the frequent, rapid resynchronizations would have otherwise been noticed since the defective channel remained online most of the time. This is one example of the ease with which a discrepancy, which might not be readily apparent at a higher level, can be noted at a low level. It is a case supportive of the subject execution monitor.

A distinction must be made between a physical error and a design error as the source of a discrepancy. As an instance of actually locating a design fault during simulator testing, one of the synchronization test cases that was applied disclosed a flaw in the verified design that was implemented in the DFCS. Specifically, the case involved two channel pairs, each synchronized for clock resetting and path traversal. But each pair continued to run without attempting to synchronize to the other pair. The resultant skew tended to yield some otherwise unwarranted voter/comparator logic trips. This occurred in flight-qualified hardware.

This problem was identified by iterating part of the design process, namely, that of reconstructing the discrepant operation in the predicate/transition network analysis simulation. Once this was done, the logic flaw and the required fix were identified. This illustrates not only the power of the diagnostic information provided by the synchronization execution monitor, but the need for better design verification test-case definition.

All of the other simulator test results merely affirmed (as intended) the correct operation of the DFCS logic as noted, for example, in figure 6-1. Affirmation was sufficient because verification is a process of confirming specified operation under the range of admissible conditions. Such confirmation was thought to have been achieved with a high degree of certainty through automated, multilevel testing, which depended crucially on the real-time execution monitors.

Despite certain inconveniences inherent in the RDFCS facility, the effectiveness of real-time execution monitors was considered excellent. There seems to be no substitute for the fidelity, precision, and conclusiveness provided in verifying fault-tolerance implementation.

As shown here, the execution-monitor testing approach should be supported by rigorous, early design verification as described in Barton, Mulcare, and LeBlanc, October 1985. Essentially, the same monitor criteria and logic model can be used both for design verification in pure simulation and for implementation verification in a system simulator. The interplay of these two assurance

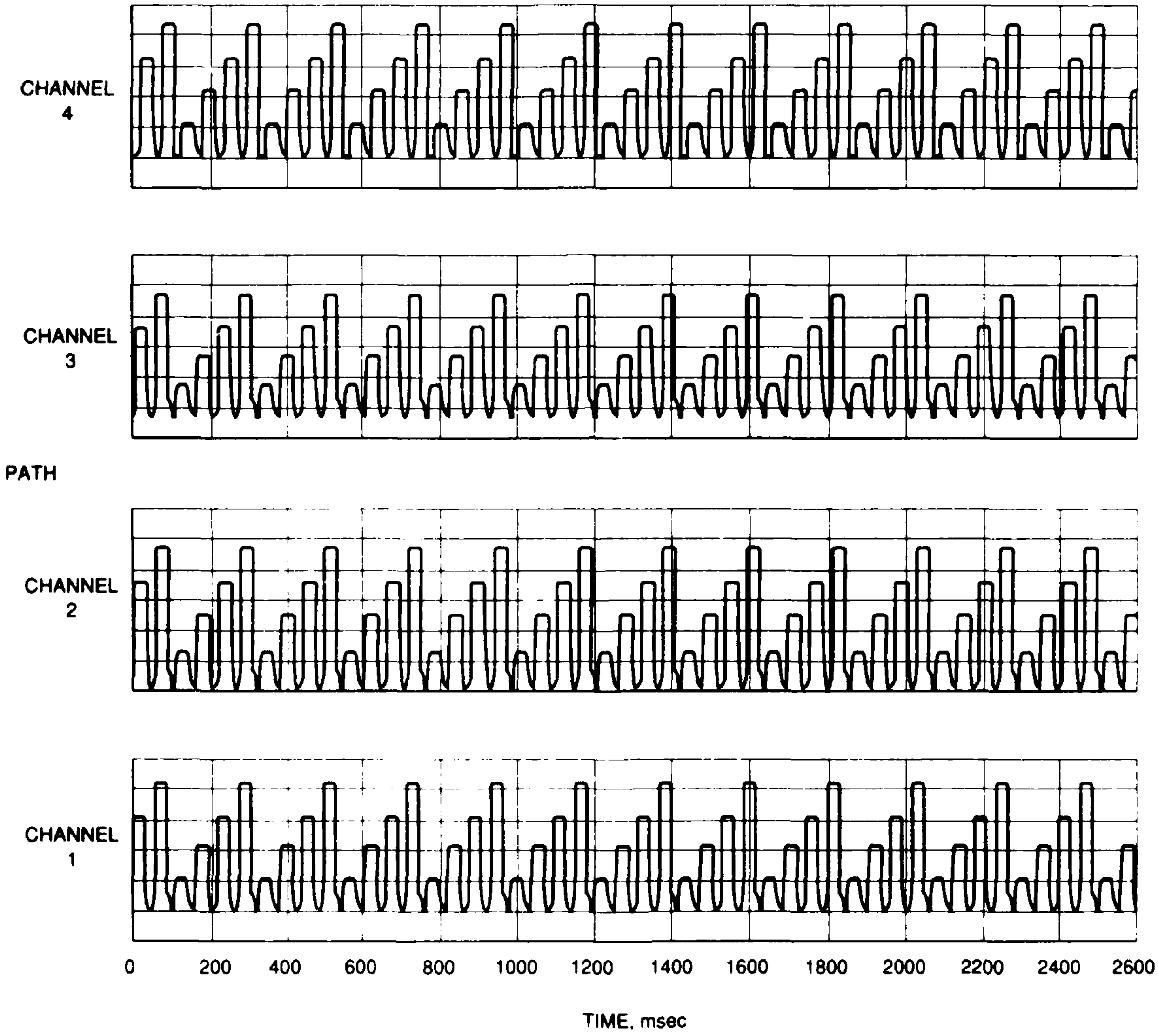


FIGURE 6-1. CROSS-CHANNEL SYNCHRONIZATION TIME-HISTORIES

activities, explicitly connected through the same precise criteria, tends to maximize confidence in the integrity and feasibility of system fault tolerance. This is fortunate, for generally the greatest source of fault-tolerant system unreliability is the fault-tolerance mechanisms themselves (Driscol, 1985).

The system state monitor aids in the interpretation of the synchronization monitor results. It can also be related to the status of DFCS components other than the flight computers. Moreover, the observed logic states can be readily correlated with flight software path traversals in an integrated testing strategy. In the interest of test productivity, comparable low-level monitoring of functions associated with different path traversals could be accomplished simultaneously. Multilevel testing would then be complemented by multifunction testing.

In summary, the demonstration of the execution monitors supports the addition of certain features to system simulators to facilitate the fault-tolerant architecture testing described. Moreover, such changes in the composition and use of system simulators appear to be a DFCS trend. As another example, similar or complementary low-level testing features have also been shown to be most valuable in the task of statistically calibrating low-level computer hardware fault-detection capability through intensive automated testing (Bensen, Mulcare, and Larsen, 1987).

# BIBLIOGRAPHY

Barton, L. A., D. B. Mulcare, and R. J. LeBlanc, "Predicate/Transition Network Analysis of Redundant Channel Synchronization," Computers in Aerospace V Conference, October 1985.

__________, "Predicate/Transition Analysis of Redundant Channel Synchronization," AIAA Paper 85-6020P, 1985.

Bensen, J. W., Development and Implementation of the Real-Time Six Degree of Freedom Airplane Simulation for the Reconfigurable Digital Flight Control System, Report Contract NAS2-10270, December 1981

Bensen, J. W., D. B. Mulcare, and W. E. Larsen, Hardware Fault Insertion and Instrumentation System: Experimentation and Results, DOT/FAA/CT-86/34, March 1987.

Boehm, B. W., "Verifying and Validating Software Requirements and Specifications," IEEE Software, January 1984.

Defeo, P., D. Doane, and J. Saito, An Integrated User-Oriented Laboratory for Verification of Digital Flight Control Systems: Features and Capabilities, NASA TM-84276, 1982.

Driscol, K. R., "Reversion, A Response to Generic Faults," AIAA Paper 85-1981CP, 1985.

Goldberg, J., General Concepts of Validation. Methods for Fault-Tolerant Avionics and Control Systems, March 1979.

Larsen, W. E. and A. Carro, "Digital Avionics Systems: Overview of FAA/NASA/Industry-Wide Briefing," 7th AIAA/IEEE Digital Avionics Systems Conference December 19[illegible]

McCabe, T. J., "A Complexity Metric," IEEE Transactions on Software Engineering, December 1976.

MIL-F-9490D, General Specification for Design, Installation, and Test of Piloted Aircraft Flight Control Systems, U.S. Air Force, 6 June 1975.

Mulcare, D. B., L. E. Downing, and M. K. Smith, Quadruplex Digital Flight Control System Assessment, DOT/FAA/CT-86/30, November 1987.

Mulcare, D. B., W. G. Ness, and R. M. Davis, "Analytical Design and Assurance of Digital Flight Control System Structure," AIAA Journal of Guidance, Dynamics, and Control, May-June 1984.

Ness, W. G., et al., *Integrated Assurance Assessment of a Reconfigurable Digital Flight Control System*, DOT/-FAA/CT-82/154, April 1983.

Reed, J. E. and E. M. Boothe, "Digital Avionics, Active Controls, and the FAA: Advanced Integrated Flight Systems (AIFS)," *2nd AIAA/IEEE Digital Avionics Systems Conference*, November 1977.

AC 25.1309-1, *System Design Analysis*, September 7, 1982.

Wensley, J. H., Design for Validation. *Validation Methods for Fault-Tolerant Avionics and Control Systems*, March 1969.

# GLOSSARY

ANALYTICAL ROOT SOLUTION. Information obtained from the roots of the characteristic equations of the airplane model such as short-period frequency response.

ANGLE OF ATTACK. Angle between the longitudinal axis of an aircraft and the direction of movement.

ASSURANCE ASSESSMENT. Procedures whose purpose is to ensure that a proposed system functions according to design specifications.

BROADCAST. Transmission of messages to all terminals without reference to the identification of the receiving station or terminal.

CHORD. The straight line segment intersecting or touching an airfoil profile at two points.

DECOUPLED MANEUVERS. Changes in an aircraft's direction and attitude in one axis without affecting direction or attitude in other axes.

DESIGN ERROR. A functional flaw resulting from a misinterpretation of the specifications of the system.

DOUBLE FAIL-OPERATIONAL SYSTEM. A quadruplex (or higher) redundant flight control system which is designed to incur failures in two redundant lanes (or channels) before it fails.

DUAL-DUAL ARCHITECTURE. Two parallel dual computers with a voting plane at the output of each dual computing lane.

ENVELOPE LIMITING. General or additional limits imposed on the structural, "g" limits, speed, attitude, etc. of the aircraft. In some cases, envelope limiting imposes additional constraints on the envelope that cannot be exceeded regardless of pilot inputs.

ERROR. A mistake in specification, design, production, maintenance, or operation of a system causing undesirable performance.

EVENT, EXTREMELY IMPROBABLE. An event with a probability of occurrence on the order of $10^{-9}$ or less.

EVENT, IMPROBABLE. An event with a probability of occurrence on the order of $10^{-5}$ or less.

EVENT, PROBABLE. An event with a probability of occurrence greater than $10^{-5}$.

FAILURE. The inability of a system, subsystem, unit, or part to perform within specified limits.

FAILURE, HIDDEN. A failure that is not manifested at the time of its occurrence.

FAULT. An error in the operation of a system.

FAULT, HARD. A defect in the hardware or software of a digital control system that permanently affects some functional performance of the system.

FAULT, SOFT. A transient defect in the software of a digital flight control system that can be overcome by error-correctable code or by recycling of power to the computer system.

FAULT INSERTION. A testing technique used to obtain information about data latency and built-in test coverage of a digital flight control system.

FAULT TOLERANT. Software which continues to operate satisfactorily in the presence of faults.

FAULT TREE ANALYSIS. A top-down deductive analysis that identifies the conditions and functional failures necessary to cause a defined failure condition. The fault tree can be used to establish the probability of the ultimate failure condition occurring as a function of the estimated probabilities of contributory events.

FLIGHT CODE. The application software of the digital flight control system.

FLIGHT-CRITICAL. A description of functions whose failure would contribute to or cause a failure condition preventing the continued safe flight and landing of the aircraft.

FLIGHT-ESSENTIAL. A description of functions whose failure would contribute to or cause a failure condition which would significantly affect the safety of the airplane or the ability of its crew to cope with adverse operating conditions.

FLIGHT-PHASE CRITICAL. A description of functions which are critical only during certain phases of flight.

FLY-BY-LIGHT. Flight control system where fiber optics carry the signal.

FLY-BY-WIRE. Flight control system with electric signaling.

GROUND EFFECT. Increase in aircraft lift when operating near the ground.

MEAN AERODYNAMIC CHORD (also mean chord). The chord of an airfoil whose length is equal to the area of the airfoil section divided by the span.

NEGATIVELY STABILIZED. Aircraft design in which the point of effective lift is aft of the center of gravity.

POINT-MASS SIMULATION. Same as state variables airplane simulation (q.v.)

POSITIVELY STABILIZED AIRCRAFT. Aircraft design in which the effective point of lift is forward of the center of gravity.

PREDICATE/TRANSITION NETWORK. A bipartite graph (a type of linear graph) to model concurrency between redundant concurrent events. Basically a modified generalized Petri net.

QUADRUPLEX ARCHITECTURE. The use of four separate lanes (or channels) of computer redundancy. Each lane can fail separately providing a fail-operational squared capability for the digital flight control system.

RELAXED STATIC STABILITY AIRCRAFT. An aircraft whose center of gravity is behind the wing's point of effective lift.

RELIABILITY ANALYSIS. A means of determining the probability of failure in a system. Military flight-critical systems typically are required to have reliability levels of $10^{-5}$ to $10^{-7}$, whereas civil flight-critical systems have reliability levels of $10^{-9}$ or less.

STATE-VARIABLE AIRPLANE SIMULATION (also point-mass simulation). Fixed aerodynamic variables are used in the solution of the equations of motion of the model instead of using look-up tables in which each aerodynamic derivative varies with airspeed, altitude, etc. The model performance is only accurate at or near the point in the flight envelope for which the variables are chosen.

STATIC MARGIN. The degree of instability in a relaxed statically stable airplane.

SYSTEM EXPOSURE TIME. The period during which a system may fail. This period extends from the last verified proper functioning to the completion of the next required performance.

TIME CONSTANT. Time required to double amplitude of the divergent real root in the pitch axis of the aircraft model.

TRANSPARENT RECOVERY. Correcting a soft fault without interrupting the system's intended performance.

VALIDATION. Demonstration and authentication that a final product operates in all modes and performs consistently and successfully under all actual operational and environmental conditions founded upon conformance to the applicable specifications.

VERIFICATION. Demonstration by similarity, previous in-service experience, analysis, measurement, or operation that the performance, characteristics, or parameters of equipment and parts demonstrate accuracy, show the quality of being repeatable, and meet or are acceptable under applicable specifications.

## ACRONYMS AND ABBREVIATIONS

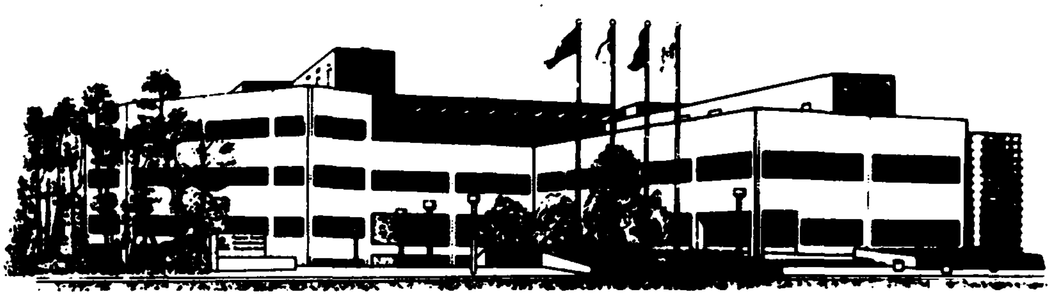
| | |
|---|---|
| AC | Advisory Circular |
| AFBW | Augmented Fly-By-Wire |
| AOA | Angle of Attack |
| CAPS | Collins Adaptive Processor System |
| DFCS | Digital Flight Control System |
| FAA | Federal Aviation Administration |
| FAR | Federal Aviation Regulation |
| FBW | Fly-By-Wire |
| FCC | Flight Cnntrol Computer |
| FCS | Flight Control System |
| MAC | Mean Aerodynamic Chord |
| MDICU | Modular Digital Interface Conversion Unit |
| MTBF | Mean Time Between Failures |
| MUX | Multiplexer |
| RDFCS | Reconfigurable Digital Flight Control System (facility) |
| RSS | Relaxed Static Stability |
| SAS | Stability Augmentation System |

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II DIGITAL SYSTEMS VALIDATION

## CHAPTER 5
## ADVANCED FAULT INSERTION AND SIMULATION METHODS



**PREPARED BY:**

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

**PREPARED FOR:**

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

## NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# CHAPTER 5

# ADVANCED FAULT INSERTION AND SIMULATION METHODS

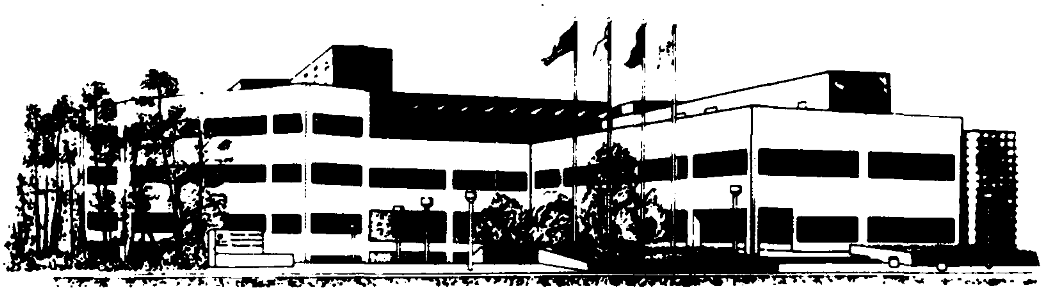
(Not included as of March 1989)

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 6
## DIGITAL DATA BUSES FOR AVIATION APPLICATIONS



**PREPARED BY:**

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

**PREPARED FOR:**

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

## NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# PREFACE

Digital data buses are used extensively in the current generation of civil aircraft. These buses are used in flight control and avionics applications to transfer data and to perform complex calculations. At the present time, the Federal Aviation Administration (FAA) has no published criteria or procedures for evaluating these complex systems, other than the general characteristics described by Federal Acquisition Regulation (FAR) 25.671, FAR 25.901, FAR 25.1309, and special conditions established by each unique aircraft type certification board.

This gap is being filled in two ways. First, standards have been developed for each major type of data bus, with the consequence that evaluation of a candidate data bus architecture can take place by comparing the "as-built" functional characteristics and system operation against the requirements published in the standards. Second, data collection, a necessary part of implementing digital data buses in new and derivative aircraft, has been an ongoing activity for the last 3 to 5 years. Information, data, and "lessons learned" from ongoing inspection, analysis, and documentation activities associated with certification testing for the Boeing 757/767 and other aircraft which use Aeronautical Radio, Incorporated (ARINC) 429, Military Standard (MIL-STD) 1553B, and General Aviation Manufacturers Association (GAMA) Avionics Stardard Communication Bus (ASCB) data buses are providing guidelines and criteria for evaluation and certification of the next generation of aircraft.

This body of standards and experience is the topic of this tutorial. The first two sections ("Introduction" and "Data Bus Architecture and Topology") provide an overview of major characteristics of data buses in general. These sections include necessary background information for understanding data buses and why they are used. Descriptions of major characteristics applicable to all data buses are also included.

The third section ("Current Aviation Buses"), summarizes current and accepted standards and requirements for five of the most commonly used aviation-oriented data buses. This section is organized to enable efficient access to specifications required to evaluate documentation presented for data bus certification. The final two sections of the tutorial ("Bus Performance Considerations" and "Fiber Optic Data Bus for Avionics Integration") address major performance requirements, applicable to all data buses, which are not currently covered by the standards. These performance requirements cover data latency, failure modes, and factors related to the use of fiber optics.

# TABLE OF CONTENTS

Section Page

TABLE OF CONTENTS (Continued)

Section Page

TABLE OF CONTENTS (Continued)

Section Page

APPENDIX

# LIST OF ILLUSTRATIONS

## LIST OF TABLES

# 1. INTRODUCTION

## 1.1. Background

Advances in digital technology have made possible greater processing power and memory capacity in smaller and smaller packages (Schmitter and Baues, 1984). Reductions in size mean that this processing capability can be located where it is needed, thus supporting the distribution of intelligence throughout the system network. In the specific case of modern civil aircraft, distributed intelligence has meant increasing numbers of distinct computer-controlled avionics, flight control, propulsion, and structural systems, with corresponding explosive growth in the volume of data being processed throughout the system.

As data processing becomes increasingly distributed throughout the aircraft, the need to support integration of this data and to allow access to it, as required, by both central and remote processors becomes apparent. Microprocessors, sensors, and servomechanisms must be appropriately interconnected to support communication and to enable fault tolerant designs to be implemented. Integrating aircraft subsystems offers numerous advantages, including the following (McSharry, 1983):

- Reduced crew workload through such capabilities as autoland and autopilot.
- Enhanced aircraft performance and capability.
- Increased hardware efficiencies (and resulting decreases in cost) through reduction in hardware duplication, complexity, and function.
- Improved flight safety through features such as flight envelope limiters.

Maximum use of common data allows the development of functional capabilities otherwise not possible. In addition, a common interface enables improvements in individual subsystems and flight tasks to be made with minimal disturbance of higher-order information transfer functions. Enhanced modularity simplifies subsystem interconnection so that retrofitting can be accomplished without the cost and complexity associated with modifying the entire system. Maintenance also becomes easier since dynamic testing of installed equipment can take place through the data bus interface by means of standardized maintenance equipment (Kiernan and Sims, 1980).

Prior to the mid-1970s, discrete subsystems passed information back and forth through analog point-to-point wire bundles. Traditionally, there has been considerable independence in the design of these subsystems. Components such as sensors were provided separately for each subsystem. However, advanced aircraft designs often require that these systems have significant interaction and a common data source. The combination of the need to integrate these systems by function and to avoid unnecessary duplication of hardware provides the impetus for developing integration techniques and supporting architectures, which both reduce the overall costs and increase performance.

The analog wire approach could not match the demands for distributed processing. It increased weight (due to the large quantity of wiring required) and economic costs, while decreasing rapid access to a database shared by all subsystems. The system designers had to develop an alternative approach: the data bus. A data bus is a system for transferring data between discrete pieces of equipment in the same complex.

Commercial and transport aircraft currently employ only single-level data bus architectures. These architectures use one of the following: (1) centralized control, (2) bidirectional information transfer system, or (3) direct-connect, unidirectional information transfer system. Microprocessor-based flight control and avionics systems (as represented by the Boeing 757/767, the Lockheed L1011-500, and the Airbus A310/A320) use data bus architectures based on either the ARINC 429-5 or the MIL-STD-1553A/B specification and standards. These architectures use shielded, twisted pair wires for the transmission medium. They interconnect microprocessors that primarily use bit slice processors. The microprocessors provide the required internal processing speed (7-14 Megahertz (MHz) clock rate) and the inherent reliability, stability, and flexibility required for flight essential and flight critical control systems. In this generation of digital systems, the individual processors are run in a bit or frame synchronized manner. The data are exchanged between redundant computers via dedicated serial data buses (either wire or fiber optic). Internally, the data are exchanged by high-speed dedicated transfer buses/backplanes.

The extensive use of existing bus structures has proven that multiplexed data transfer systems can achieve a degree of integration. The present bus characteristics are ideally matched to many intraavionics subsystem data transfer requirements. These requirements include sensor data collection, central processing, and distribution of results to peripheral areas. Continued use of bus networks for the intrasubsystem data transfer will be required.

Unfortunately, current protocols and architectures may not provide the characteristics needed to support future overall system integration requirements. The next generation aircraft will have multiple information transfer systems which require interchange of data. These systems will communicate with one another through global memory storage interface units. Consequently, such aircraft will require total airframe/system integration (on a full-time/full authority basis). With subsystems integrated in this manner, a negative change in one could possibly result in erroneous data and information being propagated throughout the entire system.

A solution to this potential problem is the development and use of an information transfer system which will efficiently interconnect, in a hierarchical order, multilevel, multiplexed buses and bus architectures. With such an approach, software-intensive, fault-tolerant executive and operating systems can be created. These operating systems provide the processing of functions required of multisystem inputs using the local terminals. A high-speed, higher-order transfer system will probably employ contention or token-passing protocols. These protocols provide each active unit (within the information transfer system structure) the capability of performing its own data processing autonomously. The responsibility for passing completed data onto the bus at the appropriate time belongs to each active unit.

Some of the more common subsystems are likely to be combined into logical units (components). New subsystems or groups of architecturally related functions will be implemented as common units. Each of the major systems will probably be designed as an integral unit. Each unit will have its own unique intra-multiplexed topological (bus) network. Each asynchronous information transfer function and topological network must be interconnected, using high bandwidth buses to create integrated data and management bases. Information flow can be directed and managed from these bases.

Data buses currently in use, such as ARINC 429, MIL-STD-1553B, and GAMA ASCB do not have the capability to handle such massive integration (see table 1.1-1). Consequently, new approaches must be developed for the interconnection of avionic subsystems to ensure the integrity of the data at all times. New bus standards are being developed to support higher-order data. The new standards use operational protocols that provide high-speed interconnection of subsystems and common sensors, sufficient subsystem independence, and fault tolerance. These protocols also distribute control of the common data bus at both the subsystem black box level and the aircraft/application level.

TABLE 1.1-1. SUMMARY OF BUS CHARACTERISTICS

| | ARINC 429 | MIL-STD-1553B | GAMA ASCB | (DATAC) ARINC 629 | SAE Linear/ Ring |
|---|---|---|---|---|---|
| Maximum Bit Rate (Hz) | 100K | 1M | 667K | 1M-2M | 10M-20M/ 50M |
| Bidirecticnal | No | Yes | Yes | Yes | Yes |
| Bus Controllers | No | Yes | Yes | No | No |
| Defined Data Formats | Yes | No | Yes | Yes | Yes |
| Low Cost Components | No | No | Yes | Yes<br>No | No |

The next generation of flight control and avionics systems architectures will be dramatically different from the current generation. It will include multiple microprocessors in each computing channel, more local processing within a processor, and the transfer of preprocessed data within the bus network. In addition, the system architectures will make use of 16/32 bit microprocessors, which will use high-speed backplane buses (running at 20-50 MHz) for internal (processor-to-processor) interfaces and exchange of data and information. Furthermore, these processors and their fault-tolerant designs will make use of global memory and functional partitioning of executive and applications software to decrease the complexity and increase the reliability of the system.

Although such objectives have yet to be realized, two data bus standards, soon to be in commercial use, will allow incremental progression towards these goals: the Digital Autonomous Terminal Access Communication (DATAC) (ARINC 629) and the Society of Automotive Engineers (SAE) linear and ring bus architectures (see table 1.1-1). These buses will be able to support the integration of avionics, flight, and propulsion systems expected to be implemented digitally in current and future aircraft. This method of implementation will allow the necessary sharing of data between subsystems.

Maximizing data availability between subsystems is in conflict with the need to isolate these systems from propagation of failures from one system to another. Therefore, the integration solution must consider the balance between the need for and type of integration, versus the flight-safety and application-criticality of each subsystem. The solution must also consider various architectural implementations within the different aircraft configurations and applications.

## 1.2. Bus Requirements

The overall advantage of integrating flight-critical subsystems (flight and propulsion controls) with other avionics subsystems can be realized only if efficient, safe, and practical methods of subsystem communication can be implemented. Items to be considered in implementing subsystem communication include the following:

- Architecture topology.
- Bus interface design.
- Interaction with the host processor (controller) and data bus interface.
- Bus protocol.
- Hardware/software failure modes.
- Fault propagation potential.
- Protection mechanisms that prohibit fault introduction or allow detection and management of faults.

The trend in data bus evolution is to implement the following general characteristics:

- Real-time data integration - current data are essential to critical flight operations.

- Protection of subsystems from propagation of failures from other subsystems. There must be an appropriate balance between integration and isolation.
- Decentralized system control.
- Standard interfaces for all equipment connected to the bus.
- Continued reductions in the use of costly hardware/software elements required in centrally controlled, data transfer systems.
- Continued dispersion of microprocessors within subsystems necessitating the interchange of processed data between subsystems.
- Generation of an aircraft database, available to all subsystems, which includes all airframe/performance parameters.
- Maximal use of common sensor data and redundant data sources.
- Further standardization of hardware/software elements by the use of other standards for interchangeability between the avionic systems and aircraft.

This tutorial examines the characteristics of avionics buses in use today. It also reviews two bus concepts proposed for use in the near future. While none of these buses has all the qualities desired for the next generation, the newer network buses offer the greatest potential match with the technology anticipated for the next generation of airframes and avionics.

Data and information for avionics systems integration can be successfully transmitted using these existing or other proposed bus structures. However, each bus has limitations, which must be considered when assessing its suitability for use in a specific application.

Before addressing the specific performance characteristics of the five buses, the topic of bus architecture and topology needs to be considered to:

- Identify the influence of physical structure on data bus performance.
- Understand the impact of dispersed locations of applications processors on computational capability and system flexibility.

## 2. DATA BUS ARCHITECTURE AND TOPOLOGY

### 2.1. Introduction

Data bus architecture and topology refers to the physical layout of the bus, (i.e., the organization of individual components attached to the buses). There are three levels of organization:

- Individual component.

  The primary purpose of a data bus is to allow individual components to transmit and receive relevant data. Each component performs a function. During the time it performs the function, it may need to receive data from or send data to one or more other components. For example, a Flight Control Computer (FCC) requires sensor data as input, performs a set of functions or equations using that data, and then sends commands to actuators or other avionics systems. Each component, therefore, requires an interface compatible with the physical structure of the bus.

- Individual bus.

  An individual bus is a topological configuration that allows the exchange of information between two or more individual components. The individual bus can support a minimum of two components up to the maximum capacity authorized by the bus architecture or structure. A specific bus may integrate related subsystems, which perform similar tasks ("the navigation bus") or integrate all subsystems ("the system bus"). Consequently, the complexity of individual buses can vary.

- System level.

  When multiple buses are used, a system level is required to integrate the individual buses. The extent of this integration depends on the degree of overall system integration required and the demands of the overall architectural design. The system level bus ensures that data are distributed to all levels that need the data at the proper time.

Each of these levels is described in more detail below.

### 2.2. The Individual Component

The generic structure of the bus/box interface is shown in figure 2.1-1.

Bus isolation refers to the physical attachment of the component to the bus medium. Typically, this attachment is accomplished by either direct coupling or transformer coupling. Direct coupling is used with short lengths of wire (normally one foot or less) with the result that impedance mismatches are not

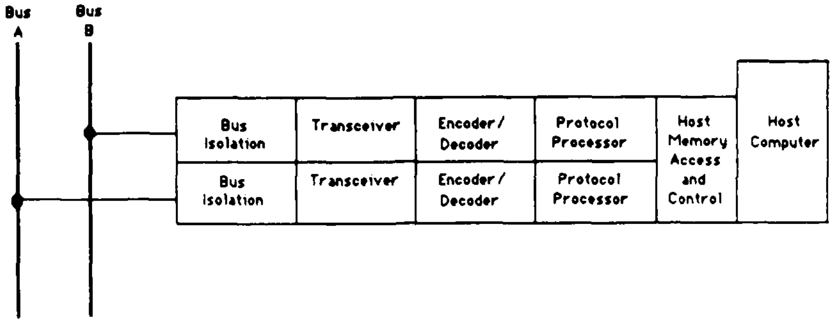


FIGURE 2.1-1. INDIVIDUAL SUBSYSTEM STRUCTURE

critical. Transformer coupling is used with longer lengths of wire (up to 20 feet) to achieve the specified signal-to-noise ratio and system error rate performance, and to maintain the proper impedance balance on both sides of the transformer over the longer lengths of connecting cable.

The transceiver is a combined transmitter and receiver. It is responsible for the interface between the digital data provided by the component and the analog format of the bus. The receiver element also has the task of monitoring the data sent along the bus until it detects "its name". Information intended for the component is detected and picked up by the receiver. The transmitter, in contrast, places information on the bus. Additional functions of the transceiver are to provide clock generation (ensuring that data are introduced to the bus at the correct time) and to evaluate received data for errors.

The encoder/decoder converts the digital data provided by the component into an analog format that is compatible with the bus. It also converts the analog data removed from the bus into a digital format. Since data buses support only serial data transfer while the processors expect parallel data, the encoder/decoder must provide serial/parallel data conversion.

The protocol processor adds or removes protocol information (such as error correcting codes) from transmitted messages. The processor is also responsible for checking the accuracy of the data coming from the bus. In evaluating data transmission protocols, the error detection and correction techniques, which could be used by the protocol processor, include Vertical Redundancy Check (VRC), Longitudinal Redundancy Check (LRC), and Cyclic Redundancy Check (CRC).

VRC appends one additional overhead bit (a "1" or a "0") to a data word to implement either odd or even parity. VRC does not detect double bit errors. LRC views a frame as a block of characters and appends an additional character consisting of the parity bit for each bit position in the character. Even when used with VRC, some patterns of even number errors remain undetected. CRC generates a frame check sequence for a frame, which is exactly divisible by some predetermined number. The frame check sequence may be verified at both ends of the transmission. Only rare combinations of errors remain undetected with this system.

Forward error correction codes are used when the receiver alone corrects data errors. The codes are calculated and transmitted along with the data. For acceptable correction, data rates are reduced by at least 50 percent. Backward error correction (retransmission) is used to resend messages when the receiver signals the transmitter that an error occurred in the transmission.

In some cases, the protocol processor translates and implements the type of message (command, status, data) and the requirements for special actions. When a bus controller is not used, two protocols may be required. The first protocol is the data transmission protocol itself. The second gains access to the bus in order to transmit data.

Host memory access and control have the capability to interrupt the main processor as required, without waiting for the response cycle through a hard-wired Direct Memory Access (DMA) channel.

The host computer is the component that actually produces data. Its functions include computation, management, and instruction. Once the host computer has completed its functions, it may request data from the bus or send its own already-processed data to the bus.

## 2.3. Single Bus Architectures

To achieve orderly transmission and reception of data, rules must be established for individual components to gain access to the bus network. These rules depend on the basic topological structure of the bus network itself. To date, the following structures have been used:

- Point-to-point.

- Linear.

- Star.

- Ring.

Figure 2.3-1 (Schmitter and Bauss, 1984) shows three of the above structures. The point-to-point topology is not included in this figure. It is similar to the linear bus except that each component is individually connected (by one or more independent wires) to other components within the system. There is no competition in gaining access to the transmitting medium, because each component is physically linked by its own wire to every other component to which it transmits. On the other hand, if a hard-wire connection does not exist, the components cannot exchange data as they would in the case of a shared, common bus. With this concept, a single transmitter can broadcast to all receivers simultaneously as long as the receivers are connected to the same wire.

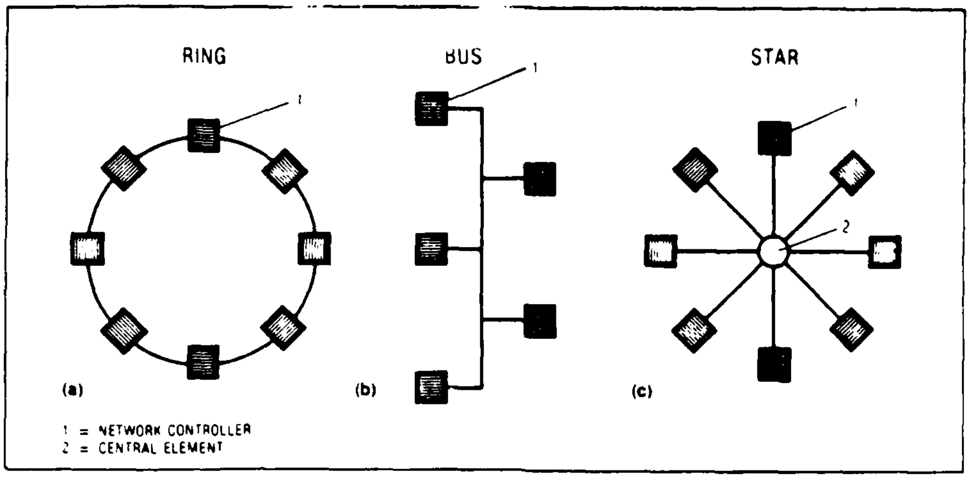


FIGURE 2.3-1. SINGLE BUS ARCHITECTURES
(from Schmitter and Baues, 1984)

With the linear bus concept, all components are attached to a common bus medium that contains multiplexed data operating in a half-duplex mode. A linear bus can be governed in either of two modes:

- By means of a centralized bus controller, which initiates information transfers to (from) specified components in a command (response) mode.

- Through decentralized operation using contention logic where a transmitter, which wishes to send data, waits until there is an opening on the bus.

The ring bus concept provides an easy method of joining together any number of stations, up to the specified limit of the addressing field, due to its use of simple point-to-point links.

With the ring bus, there are no restrictions with respect to the following:

- The minimum number of stations (above two).

- The physical or logical position of a station. (Note: the inherent token addressing dispenses with the need to have sequential addressing for speed.)

In addition, the point-to point links allow the use of any medium defined in the specification - including the possible use of mixed media (i.e., wire and fiber optic).

The star bus topology always requires a central bus controller as the active element with peripheral processing accomplished by the other application processors (boxes) attached to the central element. Star topologies are particularly suited for fiber-optic coupled systems as a result of the development of the star fiber optics couplers and the nature of the optics required.

## 2.4. The System Level

A single bus may integrate the processing of all the components comprising the vehicle system, or it may be used with components performing related functions. The former is an example of a parallel bus (see the right-hand side of figure 2.4-1). As an alternative, a hierarchical organization of multiple buses may be used (see the left-hand side of figure 2.4-1). Each set of components performing similar functions (e.g., navigation) is attached to the same bus. Integrated data produced from this bus is then passed on to a second bus, which brings together data from other low-level buses. By means of this hierarchical arrangement, progressive layers of buses, carrying ever higher levels of data, are formed. As an example, figure 2.4-2 provides a multilevel concept composed of four digital information transfer bus structures (Sensor, Management, Systems, Actuator) and one or more dedicated analog bus structures.

The sensor bus contains data that are time critical and necessary for critical system functions including:

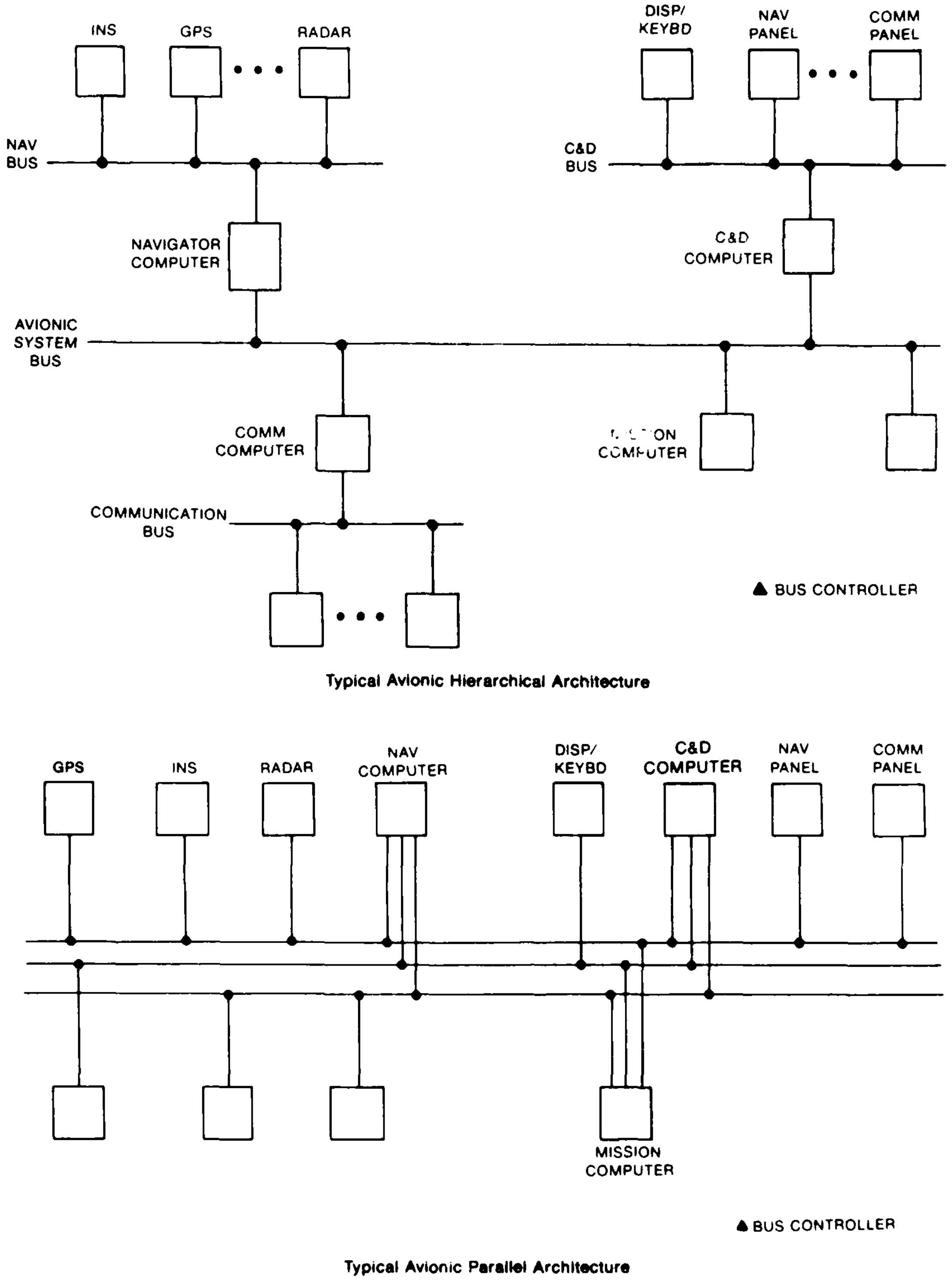
- Body accelerations and angular rates.
- Attitude angle and rates.
- Navigation and position (angles and deviations).
- Pilot inputs (column, wheel, throttle).
- Surface position (deflections and accelerations).

The data handled by the management bus are generally non-time-critical data that provide control information and system configuration. These data include the following:

- Pilot selected parameters and modes.
- Initialization data.
- Reference angles.

The systems bus transfers time-critical data that are provided (by the aircraft avionics and flight controls systems) at a constant update rate to perform mission/flight-phase oriented and automatic functions. These data include the following:

- Auto-throttle position and rates.
- Autoload (deviations, deflections, and commands).
- Attitude reference/control.



Typical Avionic Hierarchical Architecture

Typical Avionic Parallel Architecture

FIGURE 2.4-1. TYPICAL AVIONIC HIERARCHIAL AND PARALLEL ARCHITECTURES

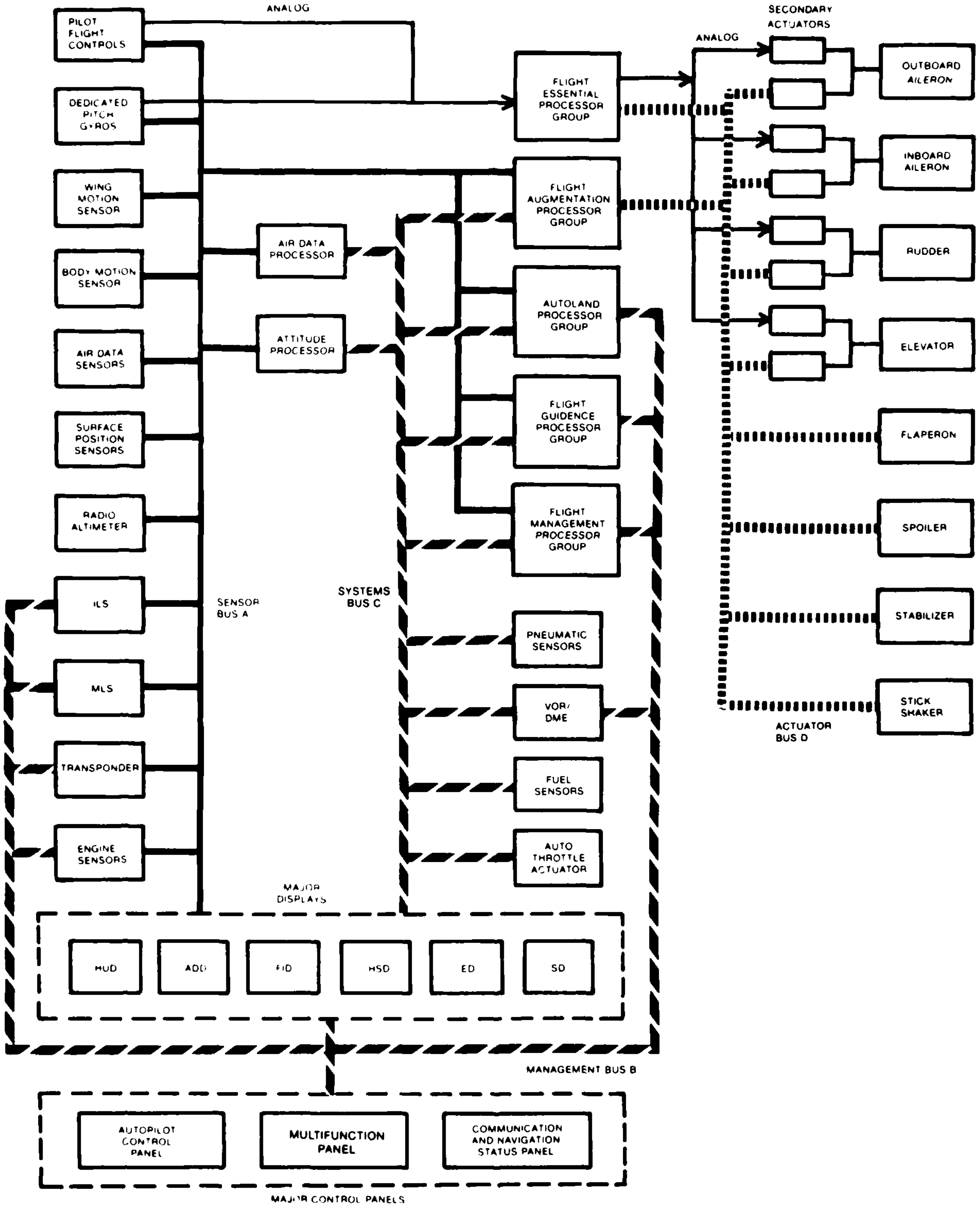


FIGURE 2.4-2. PRELIMINARY ARCHITECTURE OVERVIEW

- Flight management functions.

- Pneumatic (status/control).

- Fuel (flow/rate, quantities).

The actuator bus provides the necessary constant-update-rate data to command and feed control back to the surface controllers and tactile attitude warning devices. These data include the following:

- Deflection command/activator position (aileron, rudder, elevator, spoiler, stabilizer, etc.).

- Stability augmentation (gains/deflections).

- Stick shaker.

The analog (hard-wired) interconnections handle the flight-essential functions that include pitch rate sensors, pilot flight controls, and redundant actuators.

Early bus architectures used a parallel structure. Advances in digital technology make it possible to preprocess functions through distributed intelligence. Consequently, architectures more suitable to the sensors and actuators can be used. Onsite microprocessors can replace the central computer complex. As a result, the concept of hierarchically organized, multiple buses becomes attractive. One advantage of such an approach is that it enables easy differential treatment of critical and noncritical data simply by using different buses.

Both architectural arrangements are still in use. In general, hierarchical buses are more efficient. Data transmitted by hierarchical buses tends to receive more preprocessing than data transmitted via the parallel architecture. There is less chance of overloading system bus under hierarchical architectures. However, this also means that data tends to take longer to reach its final destination since it may have to pass through several buses.

Hierarchical buses support greater functional independence and isolation of individual subsystems. In contrast, parallel buses must carry more data but they offer a simpler architecture which allows greater reconfiguration capability.

Figure 2.4-3 (McSharry, 1983) provides two examples of the implementation of each architecture. In one case, integration is performed by means of a local bus, in the second by an avionics system bus. The avionics system bus sends out processed data while the local bus can transmit both processed and unprocessed data. The advantages and disadvantages of the hierarchical versus parallel approaches and the local bus versus system bus are summarized in table 2.4-1 (McSharry, 1983).

From the control system perspective, three integration alternatives are possible as shown in figure 2.4-4. All three cases make use of various combinations of

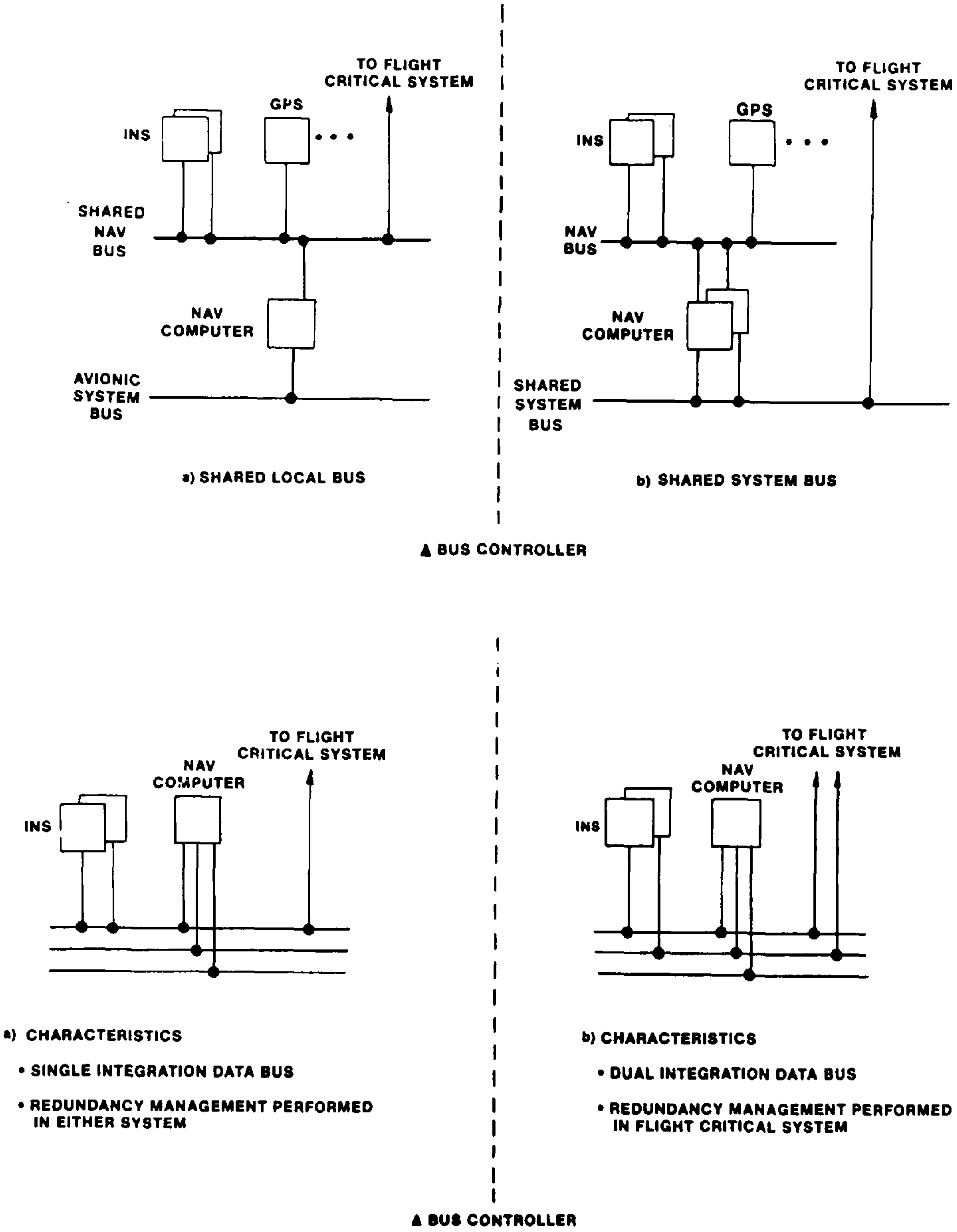
TABLE 2.4-1. COMPARISON OF HIERARCHICAL AND PARALLEL AVIONICS BUS ARCHITECTURES (adapted from McSharry, 1983)

| Hierarchical Avionics Bus Architecture | Parallel Avionics Bus Architecture |
|---|---|
| • Local Bus | • Single Bus |
| Minimum data latency | Simpler |
| Lowest intersystem impact | Greater flexibility |
| Greater isolation | |
| • Avionic System Bus | • Multiple Buses |
| Information required at more than one local bus | Higher reliability levels |
| Highest inter-/intra-system impact | |
| Greater data latencies | |

data bus structures (Sensor, Systems, Actuator, and Analog) previously referenced, and either use the FCC as a buffer between the avionics and flight control systems or connect directly to the control system bus(es) with other mission essential computers .acting as buffers. In either case, the proposed architecture or topology and the attendant integration must be defined so that one of the following conditions exist.

- Isolation (in terms of fault propagation) is maximized by integration of functions and sensor signal requirements. This may be accomplished through the use of redundant avionics buses or buses dedicated to support avionics, flight control, and other mission dependent functions within the same bus structure. This approach, however, requires higher levels of system reliability to satisfy flight safety requirements.

- Data latency is minimized by use of separated structures in which critical sensor data co-exist with the flight control and mission dependent computation function on the same bus. It may also be minimized by making optional use of existing sensor redundancy with critical sensor data being



a) SHARED LOCAL BUS

b) SHARED SYSTEM BUS

▲ BUS CONTROLLER

a) CHARACTERISTICS

- SINGLE INTEGRATION DATA BUS
- REDUNDANCY MANAGEMENT PERFORMED IN EITHER SYSTEM

b) CHARACTERISTICS

- DUAL INTEGRATION DATA BUS
- REDUNDANCY MANAGEMENT PERFORMED IN FLIGHT CRITICAL SYSTEM

▲ BUS CONTROLLER

FIGURE 2.4-3. INTEGRATION CONCEPTS
(from McSharry 1983)

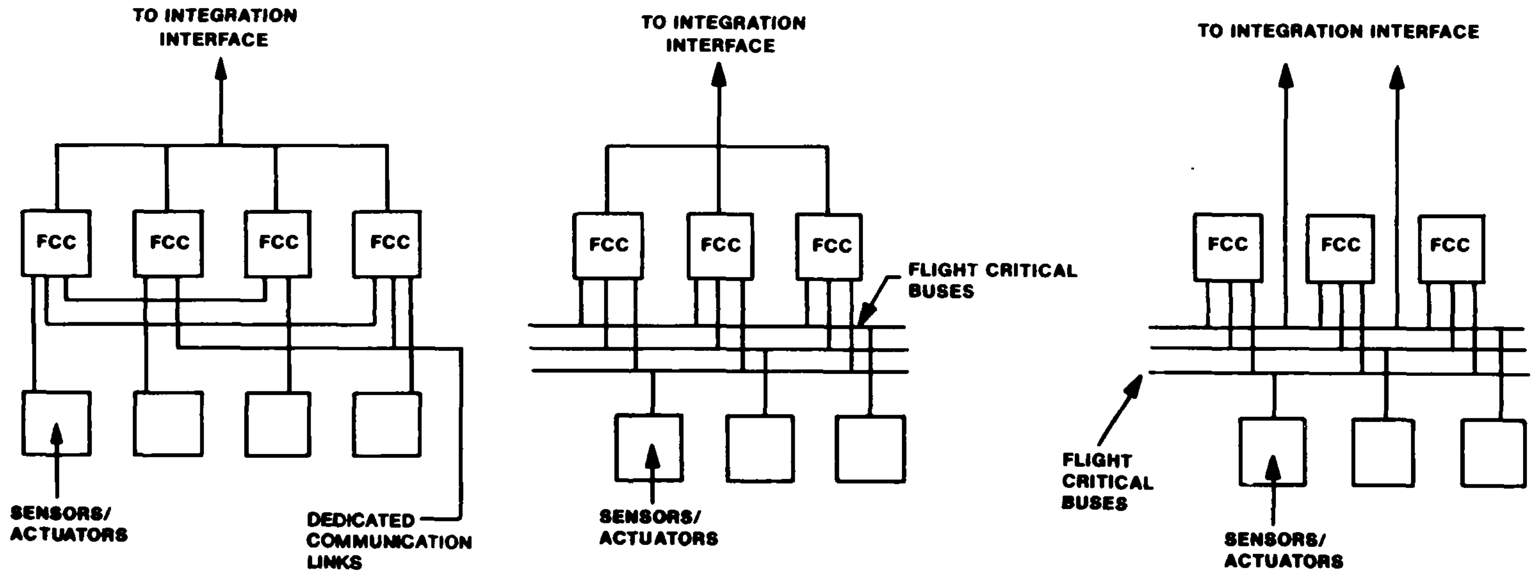


FIGURE 2.4-4. INTEGRATION CONCEPTS FOR FLIGHT CRITICAL SUBSYSTEMS

placed (through multiparty techniques) across the information transfer bus hierarchy. This approach reduces the reliability constraints on each of the various system functions. It can, however, introduce new potential failure points into the flight control and mission-dependent computation functions due to the increased complexity.

## 2.5. The Choice of an Architecture or Topology

The selection of a system architecture (including bus structure, topology, and integration concept) is based on the design requirements and the preference of the system designer, integrator, and implementor. In the concept design phase, a number of candidate architectural concepts, bus architectures, and topologies are postulated. Each is capable of satisfying system requirements within the constraints of the required performance, reliability, and safety criteria levels established by the relevant guidance documents (FARs, Advisory Circulars, and other accepted air worthiness practices). The selection of the final design for the information transfer system will ultimately be a function of selected system components, required interfaces, time-critical events and data, and various measure-of-merit attributes that drive the integrator's decisions.

The measures-of-merit and desirable bus attributes (as presented in tables 2.5-1 (McSharry, 1983) and 2.5-2 (Rich et al., 1983) are guidelines to be used by the system designer and integrator in assessing the integrity of the proposed information transfer system. Architecture, structure, protocol, and integration complexity must be considered to fully understand and evaluate the ultimate performance, reliability, safety, and airworthiness of the final design.

## 2.6. Protocol/Topology Relationships

The technical analyses leading to the selection of a topology and protocol for a given application require that topologies, protocols, media components, and configurations all be analyzed in terms of the constraints imposed upon the detailed system design, and the existing state of technology in each of these areas. Although a number of topologies and protocols currently exist, those most applicable to commercial transport are presented in table 2.6-1. As can be seen from this table, the choices for protocols are dependent upon the topologies, and the extent to which high-speed, distributed, fault-tolerant computation and passage of data are maximized in the system architecture. The topologies themselves are not likely to change in the near future, but the implementation, in terms of redundancy and hierarchical structure, will be designed to provide the critical data at the correct iteration rate with the least time delay at the lowest cost. As more and more aircraft systems are implemented with these concepts, the cost of integration (primarily Bus Interface Units (BIU)) will decrease and advances in electronics technology (at the silicon chip level) will allow additional variations which may not be feasible at the present time.

TABLE 2.5-1. MEASURES OF MERIT
(adapted from McSharry, 1983)

| Measures-of-Merit | Quantitative Measure |
|---|---|
| Flight Safety - ability to maintain control of aircraft | Probability of loss of control |
| Mission/Flight Phase Reliability - ability to satisfy mission requirements | Probability of loss of mission/ flight phase capability (i.e., Autoland, etc.) |
| Maintainability - time required to repair and frequency of repair | MTTR, MDT, MTBCF |
| Availability - ability to initiate a mission or flight phase activity/function including full-time, full-authority system (i.e., FADEC, PAS, Envelope Limiting) | Operational availability and inherent availability are usually presented as a percentage (i.e., 99%) or are given as an exposure time (i.e., two minutes). |
| Flexibility - ability to accommodate changes | Reconfiguration cost |
| Reconfigurability - ability to compute or perform mission or flight phase function in presence of failures | Dynamic reconfiguration time or redundancy default (fail safe/ fail safe) |
| Computational Capability - throughput of system computers | Total instructions executed per second |
| Data Transfer Capability - ability to send messages in a timely manner and in presence of failures | Maximum data latency, % peak bus loading |
| Pilot Interface - ability to provide cognitive information to pilot | Qualitative |
| Cost - initial procurement and life cycle cost | Dollars |

TABLE 2.5-2. ATTRIBUTES
(adapted from Rich et al., 1983)

| Attribute | Quantitative Measure |
|---|---|
| Fault Tolerance | Probability of error occurring; Reconfiguration time; Probability of propagation |
| Efficiency | Available bandwidth |
| Simplicity | Presence/absence of complexity, and complexity metric rating |
| Data Integrity | Probability of correct data transfer, and number of retries |
| Synchronous/Asynchronous | Time to respond to emergency messages/interruption |
| Adaptable to new technology; Technology Insertion | Qualitative |
| Similarity to existing bus architectures/ structures/protocols | Qualitative |
| Deterministic | Qualitative |

TABLE 2.6-1. ALTERNATIVE TOPOLOGIES AND PROTOCOLS

| TOPOLOGIES | PROTOCOLS | | | | |
|---|---|---|---|---|---|
| | COMMAND RESPONSE (ARINC 429-5) | CSMA/CD (DATAC ARINC 629) | TOKEN PASSING (SAE) | HDLC (ASCB) | TDM/CR (MIL-STD-1553B |
| Point-to-Point | X | | | | |
| Linear Bus | X | X | X | X | X |
| Star | | | | | X |
| Ring | | | X | | |

# 3. CURRENT AVIATION BUSES

## 3.1. Introduction

The first two sections of this tutorial provided a brief overview of the history and likely evolution of aviation digital data buses. This section reviews the specifications for five current and near-future avionics data bus concepts. The three data buses currently in use are ARINC 429, MIL-STD-1553B, and GAMA ASCB.

The two near-future bus concepts are as follows:

- The proposed ARINC 629 (DATAC), which is expected to be certified in the 1990s on the 7J7 and other large commercial transport aircraft.

- The two proposed SAE (Avionics System Division) High-Speed Data Bus Architectures, which are expected to be the standard for civil and, perhaps, military aviation in the year 2000 and beyond.

These five bus concepts are the only buses expected to be certified by the FAA within the next 20 years. Each bus standard reflects an ongoing attempt to develop data buses that will enable greater integration and flexibility. The proliferation of diverse data buses is due to the different needs of the developers. For example, the ASCB bus was developed by CAMA to take advantage of the large number of avionics components being developed by the general aviation avionics industry. Their bus concept was based upon the availability of low-cost commercially-available components that could be easily integrated into the low cost equipment.

Each of the buses will be discussed in terms of the following:

- Major architectural and topological characteristics.

- Protocol used.

- Design specifications.

- Major documents describing the bus and its specifications which can be consulted for additional information.

A separate appendix (appendix A) has been included to explain and define the various modulations, signaling methods, and data code waveforms that are commonly used for these digital data buses.

## 3.2. ARINC 429

### 3.2.1. History

The ARINC 429 bus standard was the first standard developed for the transfer of digital data between avionics system elements in civil aircraft. Created during the mid to late 1970s by the air transport industry (the airlines, avionics manufacturers, airframe manufacturers, and the FAA) to meet the emerging need for distributed intelligence and communication between avionics subsystems, the ARINC bus quickly replaced analog point-to-point wiring systems which were prevalent at that time. Currently, the ARINC bus standard represents the type of bus used in most civil aircraft manufactured during the past decade. A schematic representing the basic organization of the ARINC bus is shown in figure 3.2-1.

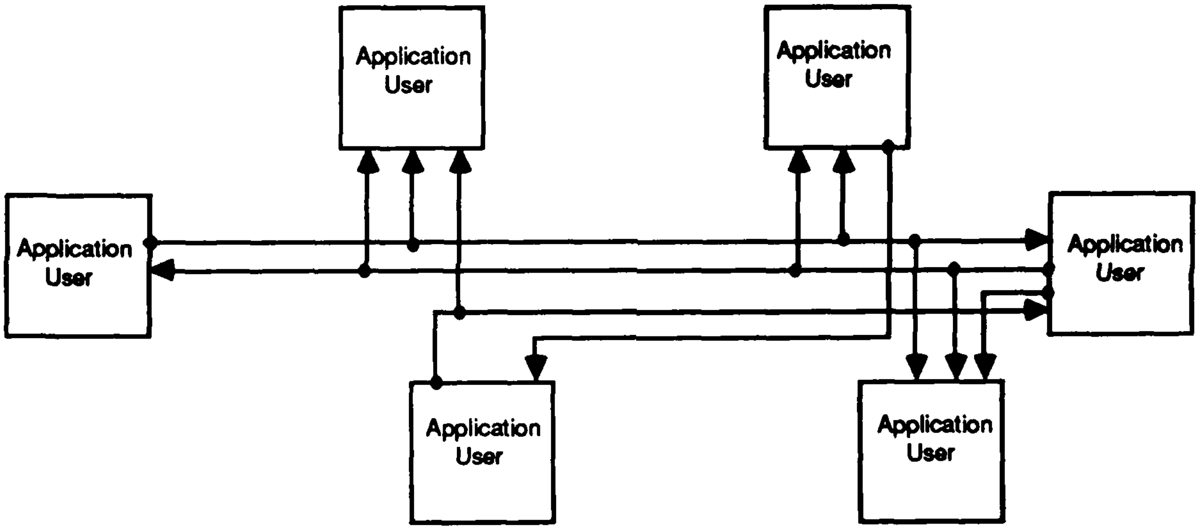


FIGURE 3.2-1. GENERIC ARINC BUS LAYOUT

### 3.2.2. ARINC 429 General Characteristics

General characteristics of the ARINC bus include the following:

- Relatively low-speed, high-reliability data transfer.

- Two data rate options (Note: High and low rate messages cannot be combined on the same bus):

  High-speed (100K bits per second (bps)) - Low-speed (12K to 14.5K bps).

- Unidirectional, asynchronous, serial data transfer.

- Data transfer by means of a single twisted, shielded pair of wires.

- Simplex data transfer only:

  Each component that needs to talk to other components has a wire going to the other components from its transmitter.

  Each component that needs to receive data from other components has a wire from that component to its receiver.

- Transmission by "broadcast" mode: receivers are not required to respond that data has been received (although they frequently do).

- Each transmitter able to send to up to 20 receivers.

- Data encoded in binary or binary-coded decimal.

- Data words composed of 32 bits, including label, word type, and a parity bit.

- Transmission accuracy determined by a single parity bit. Data reasonableness checks may also be performed.

### 3.2.3. ARINC 429 Protocol: Command Response

The ARINC 429 bus uses a Command Response (CR) protocol. When a transmitter is ready to send data to a receiver, it first sends a "request to send" word to the intended receiver by means of the bus that connects the transmitter to the receiver. If the receiver is ready, it will respond with a "clear to send" word sent by means of a separate bus that connects the receiver to the transmitter. The data then are sent immediately after transmission of a "data follows" initial word. A "final word", used for error control, signals completion of data transmission.

Once the data have been received, the receiver will process the data in search of errors, such as parity and file size. If no errors are found, the receiver may send a "data received OK" word to the transmitter. If an error is detected, the receiver requests the transmitter to retransmit the record containing the error.

Should the receiver not be ready to accept data, it sends back a modified "clear to send" that states its lack of readiness and may also specify the maximum number of records it is capable of receiving. After 200 millisecond (ms), a "request to send" is again transmitted. If, however, no response is received from the receiver, the transmitter will repeat a "request to send" after 50 ms. If the receiver fails to respond after four attempts, an alert is raised in the system containing the transmitter.

A single message, consisting of an initial word type, such as "data follows", and any data, is defined as a "record". Up to 126 data words may be sent in a single record. A single file may contain up to 127 records. Each record should contain one of the eight initial word types:

- Request to send.

- Clear to send.

- Data follows.

- Data received OK.

- Data received not OK.

- Synchronization lost.

- Header information (used to exchange file size information without actual transmission of file data).

- Poll ("I have no information for you, do you have anything for me?")

Synchronization occurs by means of a minimum of four bit-times which occur prior to each new word. Specific descriptions of these types of words, and the kind of information assigned to each bit, can be found in the ARINC 429 specification ("Mark 33 DITS").

### 3.2.4. ARINC 429 Hardware Characteristics

Table 3.2-1 presents a summary of hardware characteristics of the ARINC 429 d^ta bus.

### 3.2.5. Major Documents

The characteristics of the ARINC 429 bus are described in ARINC Specification 429-5 ("Mark 33 DITS", April 1981).

## 3.3. MIL-STD-1553B and MIL-STD-1773

### 3.3.1. History

MIL-STD-1553B was originally developed by the military to support the integration of weapon systems. It has subsequently been used in commercial aviation for a number of systems including the Coast Guard Search and Rescue Helicopter HH-65A. Developed at the same time as ARINC 429, it represents the current generation of data buses developed for military and civilian aircraft. A schematic of the generic bus is shown in figure 3.3-1.

The proposed DOD-STANDARD 1773 DATA BUS (Fiber Optic Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus) was developed for the following purposes:

- It seeks to preserve the multiplex bus techniques which have been standardized in MIL-STD-1553B, and

- It provides guidelines for the application of fiber optic transmission techniques to the MIL-STD-1553B interconnect.

TABLE 3.2-1. ARINC 429 HARDWARE CHARACTERISTICS

| | |
|---|---|
| Transmission Medium | Twisted Shielded Pair |
| Characteristic Impedance | 75 ± 5 Ohms |
| Main Bus Length | Not Specified |
| Media Connections | Direct Coupled |
| Modulation | Baseband (TDM) |
| Signaling Method | RZ Bipolar |
| Transmission Direction | Uni-Directional |
| Transmission Method | Asynchronous Broadcast |
| Transmission Order | LSB First |
| Data Rate | 12-14.5 KHz or 100 KHz |
| Data Code | RZ Bipolar |
| Bit Error Rate | Not Specified |
| Word Error Rate | Not Specified |
| Topology | Serial Bus |
| Number of Terminals/Addresses | Less Than 20 |
| Logical Addresses | Not Specified |
| Media Access | Point-to-Point |
| Data Link Control Protocol | Not Applicable |
| Error Detection | Odd Parity |
| Synchronization | Word |
| Word Size | 32 Bits |
| Data Bits/Word | 19 Bits |
| Words/Message (Min.-Max.) | 1 |
| Word Types | Not Specified |
| Intermessage Gap Time | 4 Bit Times |
| Bus Frame Length | Not Specified |
| Bus Control Transfer Time | Not Applicable |
| Terminal Transmit Interface | Not Specified |
| Terminal Receive Interface | Less Than 20 |

### 3.3.2. MIL-STD-1553B General Characteristics

General characteristics of the MIL-STD-1553B bus include the following:

- Relatively high-speed (1 MHz bit rate), high-reliability data transfer.

- Single (redundant) pathway to connect each bus element (component) to the bus controller terminal. All equipment connected to the bus has access to information sent by means of the bus.

- Data transfer by means of a single twisted, shielded pair of wires.
- As many as 31 terminals per data bus.
- Bidirectional (half-duplex), asynchronous, serial data transfer.
- Data flow controlled by a bus controller. The controller may be a separate component or share a box with other functions.
- Redundant controllers optional (although only one is active at a time). The second controller is activated if the first controller malfunctions.
- Overhead penalty for multiple terminal and controller checking, testing, and switching functions.
- Command-response protocol.
- Data word size 20 bits. Blocks of up to 32 data words are allowed.
- Transmission accuracy determined by a single parity bit.
- Synchronization by a three-bit synchronizing field.

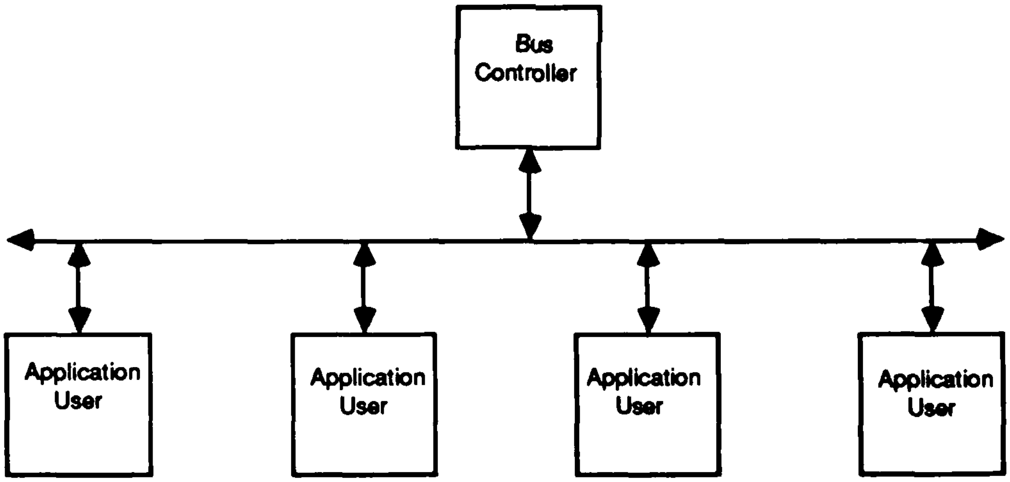


FIGURE 3.3-1. GENERIC MIL-STD-1553B BUS LAYOUT

### 3.3.3. MIL-STD-1553B Protocol: Time Division Multiplex, Command/Response

As the name suggests, data flow control for all transmissions on this bus uses a combination of Time Division Multiplexing (TDM) and command/response modes of operation. TDM refers to "the transmission of information from several signal sources through one communication system with different signal samples staggered in time to form a composite pulse train." (MIL-STD-1553 Designer's Guide, 1983, p. II-2.) With TDM, each component is assigned a pre-allocated timeslot. Consequently, an individual component knows when to transmit its data, how long it can transmit, and when to give up control of the bus to the next scheduled transmitter.

Pre-allocation of transmission slots requires that all message sequences be predefined to enable fixed schedules of data transfer. This is based on the definition of minor and major cycles. Minor and major cycles reflect the fastest and slowest iteration rates, respectively. The slowest iteration rate, which is the data required to be sampled least often, defines the time period for the major cycle. Over the course of a major cycle, all periodic bus events occur at least once and all periodic computations occur at least once. A frame is one major cycle. Within a frame, one or more minor cycles may occur as a function of the required frequency of the most rapidly transmitted periodic data.

The Multiplex Applications Handbook (1982, p. 5-4) offers the following example: "If the major frame is one second long and there are 64 minor cycles, then each minor cycle is 1/64 second or 15.625 ms long. Each periodic message would occur at least once each major frame, up to a maximum of 64 times. If a transaction needed to occur eight times per second, it must occur during one of the first eight minor cycles (64/8 = 8) and every eight minor cycles thereafter. The minor cycle in which the first message occurs is known as the 'phase', while the repetition rate is its 'period'."

Pre-allocation of timeslots means that responsibility for controlling the bus is distributed among all participating components. Since transfer of bus control can be almost instantaneous, little bus transmission time is lost. Consequently, bus utilization can, at least in theory, approach 100 percent (Rich et al., 1983). Practically speaking, this is not the case. Timeslotting is highly fault tolerant in that failure of the component currently controlling the bus does not cause a permanent disruption. Instead, the other components continue transmitting their data at their assigned slots. The only consequence is that the slot belonging to the failed component goes unfilled.

The timeslot protocol typically does not support 100 percent utilization because of problems with fault tolerance with respect to when individual message errors occur. Complete pre-allocation of slots does not allow for retransmission of messages that were not successfully transmitted initially - no slots are available for retries.

One approach for introducing message-level fault tolerance is to use timeslots that are larger than required for single-try message transmission. This leaves room for retransmission of a part of the message, if required. Clearly, this reduces the amount of message traffic supported by the bus. Providing sufficient slot time for a single retransmission of a message has the major consequence of reducing overall bus capacity by 50 percent.

Note that the message retry capability represents an "unscheduled" data transmission event. Other types of unscheduled transmission can take place during those intervals when data are not already scheduled to be placed on the bus. The bus controller can command a receiver to transmit during these intervals as required. This is an example of how the command/response mode can be superimposed on the basic TDM mode. Using the command/response mode in conjunction with TDM has two advantages: intervals when no data are scheduled to be transmitted can be filled so as to make greater use of the bus's capacity, and the controller can respond to events that do not occur regularly.

### 3.3.4. MIL-STD-1553B Hardware Characteristics

Table 3.3-1 presents the characteristics of the MIL-STD-1553B bus.

### 3.3.5. MIL-STD-1773 Hardware Characteristics

Table 3.3-2 presents the characteristics of the MIL-STD-1773 bus, which is the fiber optic counterpart of MIL-STD-1553B. MIL-STD-1773 allows for five possible coupled architectures: reflective star, transmissive star, bidirectional T, unidirectional T, and bidirectional hybrid. The star coupler may be passive or active and can be embedded within the Line Replaceable Unit (LRU) or external to the LRU. Dual speed operation of the MIL-STD-1773 data bus is being examined by a number of vendors to make better use of the bandwidth possible in the bus.

Due to the need for compatibility with MIL-STD-1553B, the MIL-STD-1773 must operate in the time domain and use Manchester II encoding. Matching the Manchester II encoding scheme of MIL-STD-1553B with a fiber optic system results in the average optical power level during each sync code or information bit equaling one-half of the on-power level. Bilevel optical Manchester modulation does have an average optical power of zero when a message is not being transmitted. Consequently, there is a low-frequency component, which has a fundamental frequency equal to the message rate, often 10 Hz or less. Fiber optic receivers are usually ac-coupled to compensate for the photodetector's electrical signal levels, which are not very large in comparison with the magnitudes of amplified drift and offset voltages. Because of this, special signal processing is needed to offset the effect of the low-frequency component.

Several techniques have been developed for dealing with this low frequency component, but these are susceptible to noise from within the system. The result is that the transmitter sections must be more efficiently decoupled from sources of noise in their equipment and must be quieter when not transmitting. In addition, because of the low input power levels to the fiber-optic receivers, the front-end electrical signal levels are much lower in MIL-STD-1773 receivers than in those for MIL-STD-1553B. To obtain satisfactory performance with the greatly reduced signal level, careful shielding is required, as well as decoupling of electrical interference on subsystem lines entering the receiver.

TABLE 3.3-1. MIL-STD-1553B HARDWARE CHARACTERISTICS

| | |
|---|---|
| Transmission Medium | Twisted Shielded Pair |
| Characteristic Impedance | 70 to 85 Ohms @ 1 MHz |
| Main Bus Length | Not Specified |
| Media Connections | Transformer Coupled |
| Modulation | Baseband (TDM) |
| Signaling Method | Biphase Level |
| Transmission Direction | Bidirectional Half-Duplex |
| Transmission Method | Asynchronous |
| Transmission Order | MSB First |
| Data Rate | 1 Megabit/Second |
| Data Code | Manchester II Biphase Level |
| Bit Error Rate | One Per $10^{12}$ Bits |
| Word Error Rate | One Per $10^{7}$ Words |
| Topology | Single Serial Bus (Redundant OK) |
| Number of Terminals/Addresses | 31 Addresses/30 Subaddresses Each |
| Logical Addresses | Not Specified |
| Media Access | Command/Response |
| Data Link Control Protocol | Not Applicable |
| Error Detection | Odd Parity |
| Synchronization | Word |
| Word Size | 20 Bits |
| Data Bits/Word | 16 Bits |
| Words/Message (Min.-Max.) | 1-32 |
| Word Types | Command, Status, Data |
| Intermessage Gap Time | 4 Microseconds |
| Bus Frame Length | Not Specified |
| Bus Control Transfer Time | Not Specified |
| Terminal Transmit Interface | Not Specified |
| Terminal Receive Interface | Not Specified |

Since optical signals cannot assume negative values, the receiver outputs, which are complementary and thus never low at the same time, cannot be used to identify the no-message state in a MIL-STD-1773 system. As a result, the no-message state and the off state of a two-level Manchester II biphase bit cannot be distinguished. In MIL-STD-1773, it is considered good practice to design fiber-optic receivers with three output states, even though the receivers have only two input states. This is done for compatibility with the outputs of wire-based receivers.

TABLE 3.3-2. MIL-STD-1773 HARDWARE CHARACTERISTICS

| | |
|---|---|
| Transmission Medium | Fiber Optic |
| Characteristic Impedance | Not Specified |
| Main Bus Length | Not Specified |
| Media Connections | Not Specified |
| Modulation | Baseband (TDM) |
| Signaling Method | Biphase Level, 2-State |
| Transmission Direction | Bidirectional Half-Duplex |
| Transmission Method | Asynchronous |
| Transmission Order | MSB First |
| Data Rate | Multiple Speed |
| Data Code | Manchester II Biphase Level |
| Bit Error Rate | One Per $10^{12}$ Bits |
| Word Error Rate | One Per $10^{7}$ Words |
| Topology | Single Serial Bus (Redundant OK) |
| Number of Terminals/Addresses | 31 Addresses/30 Subaddresses Each |
| Logical Addresses | Not Specified |
| Media Access | Command/Response |
| Data Link Control Protocol | Not Applicable |
| Error Detection | Odd Parity |
| Synchronization | Word |
| Word Size | 20 Bits |
| Data Bits/Word | 16 Bits |
| Words/Message (Min.-Max.) | 1-32 |
| Word Types | Command, Status, Data |
| Intermessage Gap Time | Not Specified |
| Bus Frame Length | Not Specified |
| Bus Control Transfer Time | Not Specified |
| Terminal Transmit Interface | Not Specified |
| Terminal Receive Interface | Not Specified |

### 3.3.6. Major Documents

The characteristics of the MIL-STD-1553B bus are described in The MIL-STD-1553 Multiplex Applications Handbook, dated February 1982.

The characteristics of the proposed DOD-STANDARD 1773 DATA BUS are described in a tutorial entitled FIBER OPTIC DATA BUSES, National Aerospace & Electronics Conference (NAECON), 19 May 1986. The specific subject is covered in the section entitled MIL-STD-1773 (C. R. Husbands, The Mitre Corporation).

## 3.4. The GAMA ASCB

### 3.4.1. History

The ASCB bus was developed, with the support of GAMA, to provide digital communications in business jets and commuter turboprop airplanes using low-cost commercially available components for the bus interface and an existing protocol (High-level Data Link Control (HDLC)). A schematic of the generic bus is shown in figure 3.4-1.

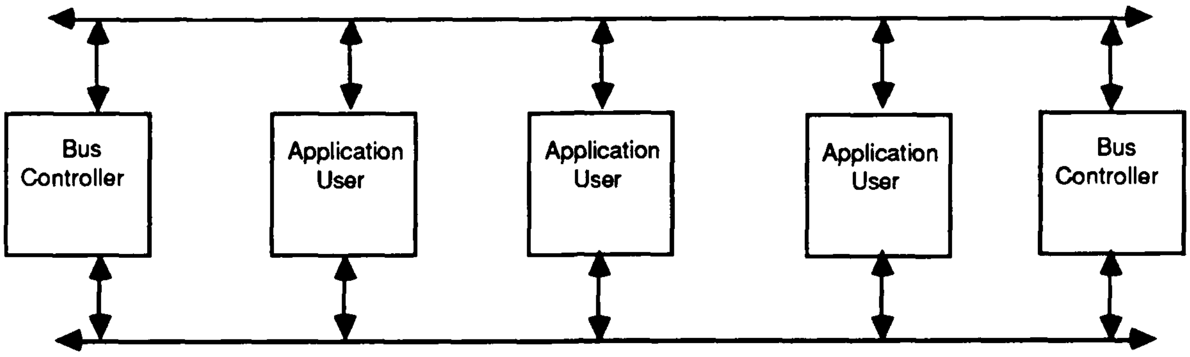


FIGURE 3.4-1. GENERIC ASCB BUS LAYOUT

### 3.4.2. GAMA ASCB General Characteristics

General characteristics of the ASCB bus include the following:

- Medium speed (0.67 MHz bit rate).
- Serial, bidirectional (half-duplex), redundant bus architecture.
- Redundant bus controllers (only one controller is active at a given time).
- Bus controller transmission on both buses simultaneously.
- Application user transmission on one bus; all application users listening to both buses.
- Support for up to 48 receivers.
- Broadcast format.
- Industry standard HDLC protocol.

- Word size of 16 bits, with up to 256 words per message.

- Low-cost interface components (transceivers, HDLC protocol chips, etc.).

- Multiple error-check capabilities, including data counters, CRC, and checksum.

### 3.4.3. GAMA ASCB Protocol: HDLC

With this protocol, transmission order is maintained by the active bus controller. An eight-frame timing cycle is used, with each frame lasting 25 ms. The bus controller requests the various users to transmit their data at appropriate intervals within the frame cycle, as required by the update rate needed for desired system performance. To prevent a user transmission from exceeding the frame time, an interlock is used.

The generic frame sequence is as follows. The active bus controller issues a start of frame word (the synchronization pattern) that announces the start of a new frame. This is followed by a frame control word, which contains information about the specific frame, including the frame number and controller identification. Any requests for user transmission complete the frame period. In this way, users can listen for information relevant to them and know when to expect that information to arrive. Similarly, each user knows when to transmit information: each user has a unique request address and response address. It listens for its address and transmits at the time stated in the frame. Users listen for their addresses on both buses. In response to a request for transmission, the user replies with its response address and the data it is required to transmit.

The transmitting user must have its data ready to transmit prior to its assigned frame. If it is not ready, the transmitter will not have enough data to fill out the frame. When this happens, the entire frame is aborted.

Synchronization is maintained by the unique eight-bit pattern that serves as both a "start-of-frame" word and an "end-of-frame" word. Each time this pattern occurs, users automatically resynchronize. This pattern, "01111110", is called a "flag". Consequently, no data sequence is allowed to contain six "1"s in a row. Whenever five successive "1"s are sent, the transmitter automatically replaces the final "1" with a false "0". The receiver then automatically replaces the false "0" with a "1". Adding and replacing these "1"s and "0"s has no effect other than to reduce the data transmission rate slightly.

### 3.4.4. GAMA ASCB Hardware Characteristics

Table 3.4-1 presents the characteristics of the GAMA ASCB.

### 3.4.5. Major Documents

The characteristics of the ASCB are described in the GAMA Specification dated February 1986.

TABLE 3.4-1. GAMA ASCB HARDWARE CHARACTERISTICS

| | |
|---|---|
| Transmission Medium | Twisted Shielded Pair |
| Characteristic Impedance | 125 Ohms |
| Main Bus Length | 125 Feet |
| Media Connections | Transformer Coupled |
| Modulation | Baseband (TDM) |
| Signaling Method | Biphase Level |
| Transmission Direction | Bidirectional Half-Duplex |
| Transmission Method | Asynchronous |
| Transmission Order | LSB First |
| Data Rate | .67 MHz ± 0.05% |
| Data Code | Manchester II Biphase Level |
| Bit Error Rate | One Per $10^8$ Bits |
| Word Error Rate | Not Specified |
| Topology | Dual Serial Bus |
| Number of Terminals/Addresses | 48 |
| Logical Addresses | Not Specified |
| Media Access | Not Specified |
| Data Link Control Protocol | HDLC (BOP) |
| Error Detection | CRC |
| Synchronization | Frame |
| Word Size | 2 Bytes |
| Data Bits/Word | 16 Bits |
| Words/Message (Min.-Max.) | 1-256 |
| Word Types | Not Specified |
| Intermessage Gap Time | 8 Bit Times (Minimum) |
| Bus Frame Length | 25 ms |
| Bus Control Transfer Time | 50 ms |
| Terminal Transmit Interface | One Bus Only |
| Terminal Receive Interface | Both Buses |

## 3.5. DATAC (ARINC Specification 629) Bus

### 3.5.1. History

The DATAC bus is being developed by Boeing in response to the ongoing changes in capabilities and complexities of avionics systems being implemented in the next generation commercial transport airplane. The DATAC bus concept is being further developed by Boeing and ARINC as ARINC Specification 629 (Multi-transmitter Data Bus) that is available (as of 1987) in draft form. The bus has already been implemented in the 7J7 for signaling, avionics, and airframe systems, and fly-by-wire. A guiding objective of the bus standard is to support ease of communication between subsystems yet avoid the problems associated with use of a central bus controller. Problems to be avoided include the potential for single point failure and the need to change the bus controller when any aspect of the bus architecture is modified. A schematic of the generic bus is shown in figure 3.5-1.

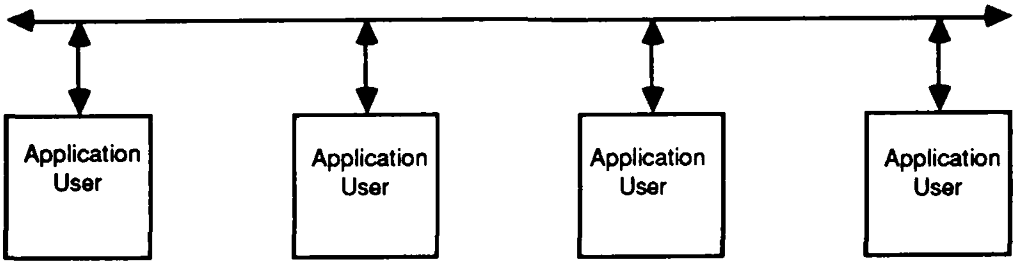


FIGURE 3.5-1. GENERIC DATAC BUS LAYOUT

### 3.5.2. DATAC General Characteristics

General characteristics of the DATAC bus include the following:

- High-speed data transfer (2 MHz bit rate).
- Shielded or unshielded twisted pair or fiber optic mode.
- Connection of as many as 120 terminals.
- Linear topology using carrier-sense multiple access/collision avoidance protocol.
- Multitransmitter implementation.
- Special current-mode coupling devices.
- Direct connection to bus through current-mode coupling devices.
- Self-monitored terminals to reduce the risk of bus failure.
- Modularity: can easily add and delete terminals without affecting overall bus functioning.
- Orderly transfer of data ensured by the protocol, rather than a bus controller.
- Carrier-Sense Multiple Access/Collision Avoidance Protocol.
- Compatibility with ARINC 429.

### 3.5.3. DATAC Protocol: Collision Detection

The DATAC protocol has no central bus controller. Instead, individual transmitters are allowed to transmit whenever they wish. Clearly, there is a strong likelihood that two or more transmitters will attempt to use the bus at the same time. Such collisions result in the transmission of distorted data from both transmitters. Consequently, both messages will have to be retransmitted. Even if a second attempt leads to successful transmission, rather severe inefficiencies in bus use will result since the time taken to send both messages could be many times longer than the lengths of the messages. Also, repeated collisions may result. As a result, use of the Collision Detection (CD) method, in its simplest form, tends to allow less than 20 percent utilization of bus capacity before bus stability becomes problematic (Rich et al., 1983). Higher utilizations radically increase the probability of collisions during a second attempt at message transmission. Once this occurs, the total traffic from the first collision, plus that from the second is thrust downstream in the overall message traffic, increasing the likelihood of additional collisions. In short, at some point the process begins cascading until all terminals in the network become involved and no successful transmissions can be performed.

Although the "pure" form of CD has some severe problems, modifications of this approach are more successful. One approach is to enable each transmitter to detect the presence of a message on the bus and, if the bus is "busy", to delay transmission of its message. This approach is known as Carrier Sense Multiple Access (CSMA). When used in conjunction with CD it is referred to as CSMA/CD and is the basis for the DATAC protocol.

With CSMA/CD the occurrence of interfering transmissions is restricted to that situation in which two terminals begin to transmit "so closely together in time" that neither has yet sensed the other's signal. This short time interval at the beginning of a message is referred to as the "collision window" and is simply due to the propagation delay of the network. The collision window is typically on the order of a microsecond in a wired network over short distances.

Requiring the following three events to occur before a transmitter is allowed to send a message again prevents collisions (Shaw, Herzog and Okubo, 1986, p. 223):

"(1) a frame time, common to all terminals on the bus, must have elapsed
(2) a sync gap, common for all terminals, must have existed on the bus
(3) a terminal gap, common for all terminals, must also have existed on the bus."

To protect against corrupted data, the receiver of the transmitting terminal monitors the transmission and checks that each label transmitted has been authorized, that each label contains the correct channel information, that the number of words allowed in that string has not been exceeded, and that the number of word strings in a message has not been exceeded. Any fault causes the transmitter to be inhibited for the remainder of that messages. It is allowed to try again on the next frame time. This continues until a certain number of successive tries are unsuccessful, at which time the terminal is permanently disabled.

### 3.5.4. DATAC Hardware Characteristics

Table 3.5-1 presents characteristics of the Boeing-developed DATAC (ARINC Specification 629) bus.

TABLE 3.5-1. BOEING DATAC BUS CHARACTERISTICS (ARINC Specification 629)

| | |
|---|---|
| Transmission Medium | Twisted Pair (Non-Shielded, Insulated) |
| Characteristic Impedance | Not Specified |
| Main Bus Length | <100 Meters (m) |
| Media Connections | Transformer Coupled (Current Mode) |
| Modulation | Baseband (TDM) |
| Signaling Method | Biphase Level |
| Transmission Direction | Bidirectional Half-Duplex |
| Transmission Method | Asynchronous Broadcast |
| Transmission Order | LSB First |
| Data Rate | 2 MHz Bit Rate |
| Data Code | Manchester II Biphase Level |
| Bit Error Rate | One Per $10^{12}$ Bits |
| Word Error Rate | Not Specified |
| Topology | Single Serial Bus (Redundant OK) |
| Number of Terminals/Addresses | Up to 120 |
| Logical Addresses | Not Specified |
| Media Access | Contention |
| Data Link Control Protocol | CSMA/Collision Avoidance |
| Error Detection | Odd Parity |
| Synchronization | Frame |
| Word Size | 32 Bits |
| Data Bits/Word | 16 Bits |
| Words/Message (Min.-Max.) | 1-4096 (256 Words/String, 32 Str/Msg) |
| Word Types | Not Specified |
| Intermessage Gap Time | 14 Bit Time Minimum (Terminal Dependent) |
| Bus Frame Length | 50 ms |
| Bus Control Transfer Time | Not Specified |
| Terminal Transmit Interface | Not Specified |
| Terminal Receive Interface | Not Specified |

### 3.5.5. Major Documents

The characteristics of the DATAC bus are described in draft ARINC Specification 629 (Multi-Transmitter Data Bus) Part 1 - Protocol Description and Part 2 - Label and Word String Definitions, both dated September 1987.

## 3.6. SAE High-Speed Data Buses

### 3.6.1. History

The newest data buses are being developed by the SAE and industry through the SAE Avionics System Division (formerly SAE/AE-9B High-Speed Data Bus Subcommittee). Under this organization, two competing bus standards are being developed: (a) High-Speed Ring Bus Standard; and (b) Linear Token Passing Bus (LTPB) Standard These two bus concepts are currently in the development stage with draft specifications having been produced (through 1988) and prototype hardware having been developed and tested. Schematics of the two buses are shown in figures 3.6-1 and 3.6-2.

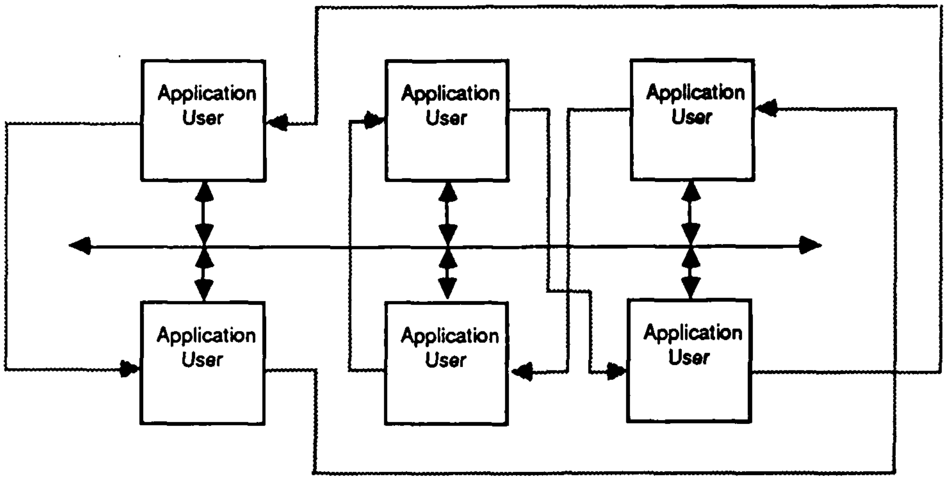


FIGURE 3.6-1. GENERIC SAE LINEAR BUS LAYOUT

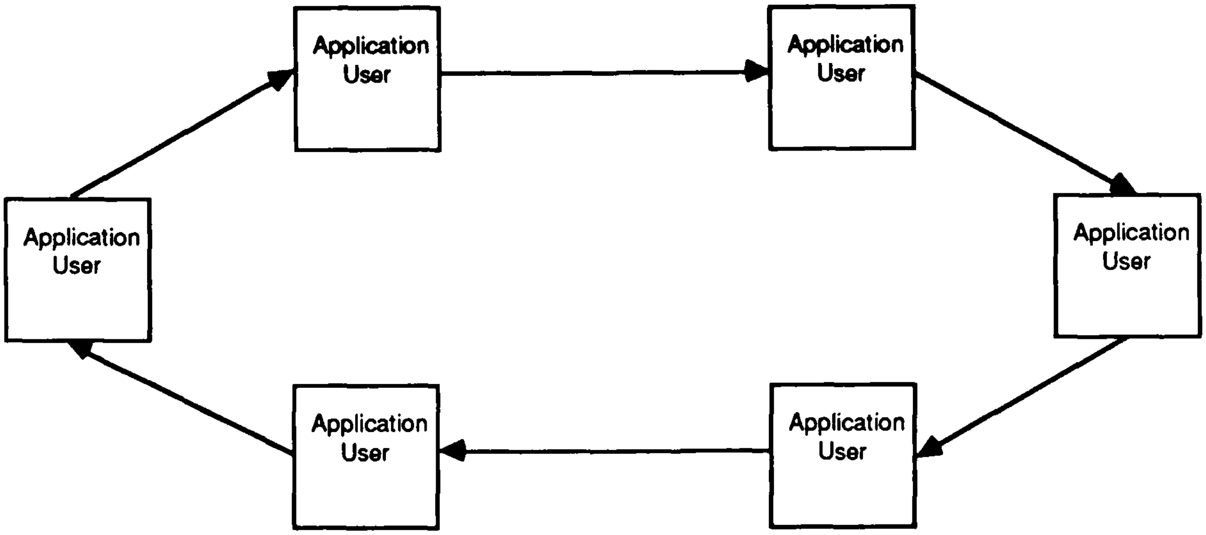


FIGURE 3.6-2. GENERIC SAE RING BUS LAYOUT

### 3.6.2. SAE General Characteristics

General characteristics of the SAE buses include the following:

- High-speed data transfer (20-40 MHz bit rate).
- Shielded or unshielded twisted pair, coaxial cable, or fiber optic media.
- Serial, bidirectional (half-duplex) data flow.
- Connection of as many as 128 physical terminals on each of four buses.
- Both broadcast and multicast modes.
- Modularity: can easily add and delete terminals without affecting overall bus functioning.
- Orderly transfer of data ensured by the protocol, rather than a bus controller.
- Word size of 16 bits (message lengths range from one word to 256 words for the linear bus; up to 4096 words for the ring bus).
- Logical addressing with $2^{16}$ addresses available.

### 3.6.3. SAE Protocol: Token Passing

Like the CD protocol, the token passing protocol also gives control of bus transmission to the transmitters themselves. Instead of a central bus controller, the currently-sending or last-sending station serves as the current controller. While acting controller, the transmitter provides the clock source for the entire bus, transmits its message, then passes a "token," a special message containing a data word which identifies the terminal which is to become the next controller. Each t' ansmitter adds "1" to the token word before passing it on. The transmitter wnich receives the token becomes the new acting controller, repeating the same process.

When the last terminal controlling the bus completes operations, a message with a non-existent token number is created and transmitted. Since there is no terminal with that token number, a brief lapse occurs in the flow of data. The token-zero terminal is responsible for timing this data lapse and assuming control of the bus after the specified period of inactivity. Thus, the system automatically restarts itself with token zero whenever control lapses regardless of the number of terminals active in the system.

A terminal attempting to use an already active bus system simply monitors the bus for a few cycles to determine the highest token number currently in use. When this terminal identifies a token number to which no other terminal responds, it adopts this number and responds the next time that token number is issued. Since this terminal responds within the appropriate time-frame, the token-zero terminal does not jump in. The token-zero terminal will restart the cycle after the new terminal has completed its operations and passed on a token to which no other terminal responds.

When a terminal has failed during a cycle and a token is offered to it, the token is ignored. No terminal takes control and bus activity ceases. The token-zero terminal detects the lack of activity and resumes control of the bus. All terminals with token numbers higher than the failed terminal are skipped. Each terminal in the system should be programmed to recognize and respond to this situation.

A terminal recognizes that something has failed in the network when more than two complete cycles have passed since the terminal received its last token offer. The terminal therefore decrements its token number by one. On the next cycle some terminal will recognize the previously ignored token and assume control. All higher numbered terminals have also decremented their token numbers and normal operation resumes. Until the ignored terminals decrement their tokens to rejoin the loop, abbreviated cycles will be run. Normal operations resume ignoring the failed terminal. If the unit recovers, it enters the loop as previously described.

This protocol works even if it is the token-zero terminal which fails, because when the token-one terminal discovers that it is being ignored, it decrements its token to zero and assumes the token-zero terminal functions. This implies that all terminals must have token-zero capabilities.

The token passing approach is highly tolerant of transmitter failure. But as was the case with the basic CD protocol, it is not as fault tolerant with respect to message errors. When a transmitter fails, not only is its data lost but also the data of all transmitters that follow the transmitter in the queue. Transmitter failure results in the transmission process starting over with the token zero terminal.

A potential problem arises because the protocol does not necessarily offer a good environment for managing unscheduled events since a terminal cannot transmit until the token is passed to it. The time between the generation of an unscheduled message and its transmission may be excessively long. Consequently, a true emergency message cannot be handled by the protocol without a scheme for assigning priorities, such as frequent polling of the source.

Another potential problem with this protocol is coping with message errors. For example, the time-out executed by the token zero terminal needs to be kept small in order to maintain high bus utilization. However, should a controller (due to extended error analysis,) pause too long before its next bus operation, the token zero terminal could interpret this as the end of a cycle and start the next cycle.

Consequently, resumption of operation by the pausing terminal could cause a collision with the traffic from the token zero terminal. When this happens, both colliding terminals believe they have failed. Should this occur, all bus activity stops until other bus transmitters recognize the problem and recover by adjusting their tokens accordingly. This may not fully resolve the problem because when the two failed terminals attempt to rejoin the network, a collision is likely to occur once again. A collision can occur either between the two "failed" systems or between one of the "failed" systems and a correctly operating system.

Rich et al., 1983 suggest that concerns about such collisions could lead to extending the interval defined for token zero time-out. Rules for testing bus activity before initiating a new cycle need to be defined. Both these rules and the token zero time-out interval need to be considered when defining the time interval used by each terminal to decide when to decrement its token. This time interval should be longer than the maximum size and may be extended as a precaution.

The SAE High Speed Data Bus Committee, for both the linear and ring buses, has recognized these problems and has formulated solutions within the protocol.

### 3.6.4. SAE Hardware Characteristics

Table 3.6-1 lists the characteristics of the SAE High Speed Ring Bus (HSRB). This system is a physical token passing ring network which connects a set of stations in a closed loop topology with a serial transmission medium. While the semantics and protocol described are independent of the data transmission rate, the HSRB is intended to operate in the range ten million to one hundred million bits per second.

Ring access is by means of a token which passes from one station to the next to provide equitable access for any given priority of message. Data are transmitted in messages from one station to the next in a unidirectional manner, starting with the sending controlling station passing through the intermediate stations to the receiving addressed station. The receiving station copies the message for its bus interface unit (BIU) user and also retransmits it on the ring. The message passes through the remaining stations until it reaches the sending station that removes it from the ring. The controlling station must then transmit a token. A station is not permitted to transmit more than one message before issuing a token. Only a station that has claimed a valid token is authorized to transmit a message for its BIU user, all other stations are constrained to repeat each message as received on the ring with the exception of setting error reporting and priority reservation bits.

The ring bus offers superior throughput capability when compared with the linear bus due to short point-to-point media links between nodes. In the area of fault recovery and reliability, the ring is less attractive due to the need for failed node bypassing using either mechanical relays or fiber optic switches. Ring reconfiguration may take up to 25 ms when bypasses are activated. In addition, a limit must be placed on the number of consecutive nodes which may be bypassed, due to a lower power budget in the short point-to-point links and the relatively high losses inherent in the bypass devices (both wire and fiber optic).

Table 3.6-2 presents the characteristics of the SAE AS-2 (Formerly AE-9B) Linear Token Passing Bus (LTPB).

The AS-2 proposed LTPB protocol involves four simple states:

- Bus Initialization.
- Normal Token Passing.
- Station Insertion.
- Station Management.

The token is passed from the lowest physical address to the highest physical address and then back to the lowest.

TABLE 3.6-1. SAE RING BUS HARDWARE CHARACTERISTICS

| | |
|---|---|
| Transmission Medium | 50 MBPS Coax, 100 MBPS Fiber Optic |
| Characteristic Impedance | 75 ohm Triax |
| Main Bus Length | 300 m required, 1000 m desired (total station separation) |
| Media Connections | Optical or Transformer Coupling |
| Modulation | NRZ-I |
| Signaling Method | Biphase Level |
| Transmission Direction | Unidirectional |
| Transmission Method | Asynchronous Broadcast |
| Transmission Order | LSB First |
| Data Rate | 10-1000 MBPS |
| Data Code | Unspecified |
| Bit Error Rate | One Per $10^{12}$ Bits |
| Word Error Rate | Not Specified |
| Topology | Ring - 2 to 128 Stations |
| Number of Terminals/Addresses | 128 Physical/512 Subaddresses Each |
| Logical Addresses | $2^{15}$ - Broadcast and Multicast |
| Media Access | Token Pass |
| Data Link Control Protocol | Token or Message Frame |
| Error Detection | CCITT-CRC-16 |
| Synchronization | Frame |
| Word Size | 16 Bits |
| Data Bits/Word | 16 Bits |
| Words/Message (Min.-Max.) | 1-4096 |
| Word Types | 4B5B Block Encoding |
| Intermessage Gap Time | Not Specified |
| Bus Frame Length | 80K Bits |
| Bus Control Transfer Time | 10 Million Data Bits/Second |
| Terminal Transmit Interface | 4 Buses |
| Terminal Receive Interface | 4 Buses |

TABLE 3.6-2. SAE LINEAR BUS HARDWARE CHARACTERISTICS

| | |
|---|---|
| Transmission Medium | Fiber Optic or Electrical Wire |
| Characteristic Impedance | 50 ohms (electrical wire systems) |
| Main Bus Length | 300 m required, 1000 m desired |
| Media Connections | Optical or Transformer Coupling |
| Modulation | NRZ |
| Signaling Method | Biphase Level |
| Transmission Direction | Bidirectional Half-Duplex |
| Transmission Method | Asynchronous Broadcast or Multicast |
| Transmission Order | LSB First |
| Data Rate | 25, 50, or 100 Mbps (Optical Bus)<br>50 Mbps (Wire Bus) |
| Data Code | Manchester Biphase II |
| Bit Error Rate | One Per $10^{12}$ Bits |
| Word Error Rate | < 1 Every 4 Hours at BIR |
| Topology | 1 to 4 Serial Linear Buses |
| Number of Terminals/Addresses | 128 Physical/256 Subaddresses Each |
| Logical Addresses | $2^{15}$ |
| Media Access | Token Pass |
| Data Link Control Protocol | Token or Message Frame |
| Error Detection | CCITT-CRC-16 |
| Synchronization | Frame |
| Word Size | 16 Bits |
| Data Bits/Word | 16 Bits |
| Words/Message (Min.-Max.) | 1-256 Required, 4K Desired |
| Word Types | Not Specified |
| Intermessage Gap Time | 10 Bit Times |
| Bus Frame Length | Not Specified |
| Bus Control Transfer Time | Not Specified |
| Terminal Transmit Interface | 4 Buses |
| Terminal Receive Interface | 4 Buses |

The worst case delay in the AS-2 LTPB is directly dependent on the maximum allowable message length. Message latency can be easily handled by implementation of system level message priorities.

In the linear bus, each component is assigned a logical token number (which may or may not correspond to the physical organization of components along the bus). A component gains access to the bus when it receives a token. On receiving the token, the component is allowed to use the bus for a pre-determined, maximum amount of time. This time limit for transmitting data is determined by the Token-Holding Timer (THT).

When the component completes its message (or times-out) it passes the token to the next higher numbered component. It is the responsibility of the passing component to verify receipt of the token by the receiving component. If, after two tries, the receiving component does not accept the token, the sending component increments the token number and tries again. This process is reiterated until all addresses are exhausted. The token is then set back to zero.

Stations are allowed admittance to the logical ring on a periodic basis. Each station contains a Ring Admittance Timer (RAT). When this timer expires and there is a gap between the local station's address and that of its successor then the token is passed to the sequential address following that of the local station. The normal token passing rules are then applied. Therefore, if any of the stations in the gap desire admittance they will be granted an opportunity during this time period.

### 3.6.5. Major Documents

The characteristics of the SAE High-Speed Data Buses are described in the two draft specifications: (a) HSRB Standard, draft dated March, 1987; and (b) LTPB Standard, draft dated April, 1987. Both of which are available from SAE, Warrendale, Pennsylvania.

# 4. BUS PERFORMANCE CONSIDERATIONS

## 4.1. Introduction

This section looks at two major types of performance considerations that affect all buses. The first part addresses problems that can arise from delays in data transmission, specifically, data latency and system delays. These are presented in order to demonstrate the potential adverse impact of delayed (i.e., old) data on aircraft system performance. In the remainder of this section, attention is then given to the problem of bus failure, including major causes and methods for reducing the likelihood of failures.

## 4.2. Issues of Latency

### 4.2.1. Types of Latency

Two types of latency affect the overall performance of a data bus: data latency and system latency. These must be considered because they can impact the performance of the avionics systems as well as the aircraft itself. For example, in critical situations such as CAT IIIa landings, latent attitude or heading data can seriously impact the pilot's ability to land the aircraft successfully.

### 4.2.2. Data Latency

Data latency is the delay from the time when a piece of information becomes available at a source terminal to the time it is received at the destination. The degree of latency is affected mainly by the architecture and the protocol of the message transmission. Hierarchical architectures, as previously defined in figure 2.4-1, are inherently subject to longer delays than are parallel architectures, due to the number of nodes (common exchange points) through which a message must pass. Node information is made available at different times at various levels of the architecture, depending on the number of nodes through which it must pass.

For example, if the FCCs control the initial transfer of the node data/status, then (depending upon the protocol) the information can be made available to application-oriented computers or other FCCs with minimum delay. The next level transfer is controlled by the application-oriented computers. Depending upon the protocol, the data will eventually arrive at the destination terminal after incurring routine delays. During this same period, the applications computer (avionics, navigation, etc.) can be providing information to other computers, within the hierarchical architecture, based upon the node data/status information it currently has available. If however, the node data/status information had been changed during an activity controlled by the other applications computers, there is a potential for error. These errors occur when one or more of the FCCs is in a node status different from the other avionics or FCC currently performing the activity.

To minimize the potential for error due to latency, the node data/status message could include a "time tag" generated when it is sent from the node select computer. When each successively higher level within the architectural hierarchy generates a message or command, it would automatically pass along the time tag of the node data/status message. When the message arrives at the various destinations, within the hierarchy, a comparison is made of the current and new node data/status values and the time tag to ascertain the validity of the command.

In general, the actual latency of a message within a given architecture is determined by the rate at which the bus structure (either autonomously or centrally controlled) allows a "sending" terminal the opportunity to "latch-on" to the bus in order to transmit its message/data. For a centrally controlled bus, to obtain the least possible (i.e., minimum) latency, the controlled bus could be configured to (1) continually poll the terminals within the bus structure, (2) respond to the service request bit in the terminal status word, and (3) initiate the terminal-to-terminal (or terminal-controller) message transfer.

An increase in the distribution of processing tasks to more specialized computers is occurring. Given this trend away from a central general purpose computer, an event-based scheduling scheme (i.e., scheduled or unscheduled system interrupt, such as a key press, a flag operation, etc.) may become a good alternative for some applications. When task scheduling is based on events rather than time, the latency of a message becomes more critical. The continuous polling technique is an effective way to reduce the message latency.

For an illustration of the event based scheduling, refer to the local display bus of figure 4.2-1. The display computer is normally operating in response to messages from the application computer. Its bus interface, which controls the local display bus, is continuously polling for keypad entry. When the keypad is pressed, a message is sent back to the display computer signaling an event to which the display computer must respond. The display computer will break out of its normal cycle, process the keypad message, and upon completion of this processing will have available keypad information that can be sent to other devices on the mission computer bus.

In this application two advantages are obtained from the event based scheduling and continuous polling. The latency of the message as it passes from a local bus to a higher level bus is minimized. Component faults in the communication system are identified early to provide time for management of the failure. For example, a simple management scheme would be to retransmit if the status response were not returned with the message error bits clear. A disadvantage of event based scheduling and continuous polling is that testing is more difficult due to the tester's inability to repeat a particular condition. When all scheduling is time based, then a repeatable test scenario can be generated. System response can therefore be accurately evaluated. When operation is based on asynchronous events, only a statistical comparison of results from multiple tests is valid.

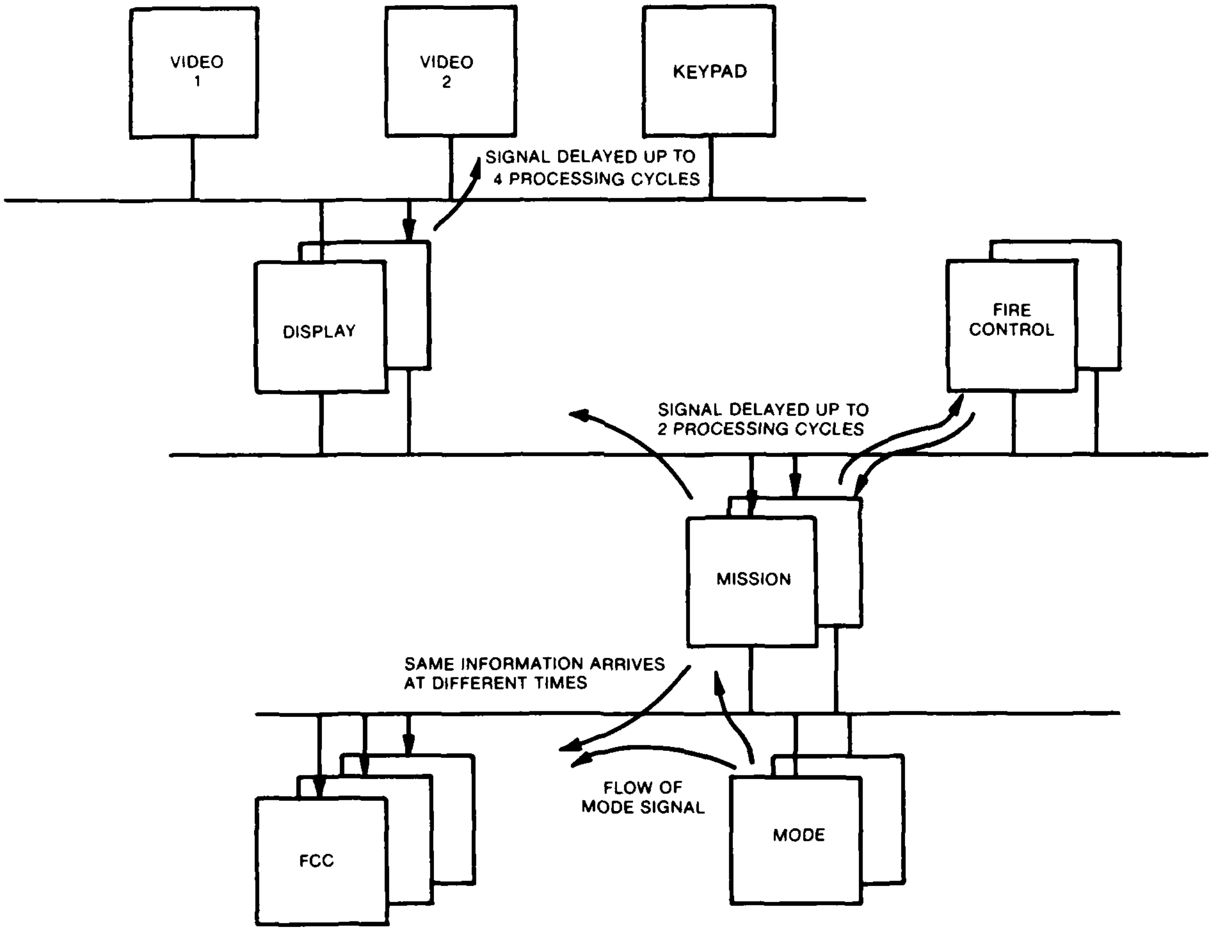

VIDEO 1
VIDEO 2
KEYPAD
SIGNAL DELAYED UP TO 4 PROCESSING CYCLES
DISPLAY
FIRE CONTROL
SIGNAL DELAYED UP TO 2 PROCESSING CYCLES
MISSION
SAME INFORMATION ARRIVES AT DIFFERENT TIMES
FLOW OF MODE SIGNAL
FCC
MODE

FIGURE 4.2-1. DATA LATENCY ILLUSTRATION IN HIERARCHIAL ARCHITECTURE

On a single hierarchical level, there are several protocols that can be used within the bus architecture framework. The choice of protocol affects message latency. For example, the use of a stationary master that polls all terminals on a regular basis provides minimum latency for a small number of terminals on the bus.

Alternatively when bus control is exchanged among a limited set of master computers, potentially greater latency is possible (depending upon the message table orientation of each master computer). If bus control capability exists in every terminal that may have a time critical message, the message latency will be in the range of several (2-4) ms. If continuous polling is done between message transmissions, latency improves; however, a large bandwidth penalty is paid. Continuous polling can only be used on buses with low activity levels.

4.2.3. System Delays

Average transfer delay is defined as the sum of delays resulting from queuing delay, access delay, and transport delay.

- Queuing Delay.

  Queuing delay is characterized by message arrivals and arrival rate. It is represented (characterized) as a Poisson Distribution. The mean queuing delay consists of the average delay incurred due to a message waiting for a previous message within the BIU to be serviced. The BIUs are effectively a single server queue, and therefore the queuing delay is a delay imposed on the user due to the BIU transmit buffer being full. This delay neglects the user/BIU message processing rate limitations and is dependent only on the message interarrival time as determined from the offered load.

- Access Delay.

  In the case of the CSMA/CD protocol, the mean access delay is determined by considering the two inherent access modes. The delay due to the random mode and the delay due to the ordered access mode are factored with the probabilities of being in their respective states and combined to equal the mean access delay.

  For the random access delay there are two components of delay: (1) delay due to the bus being busy, and (2) delay due to a collision. For the bus to appear busy, at least one other message must arrive before the message that encounters the media active state. Therefore, the probability of the bus being busy is the probability of two or more arrivals within the same time window.

  The probability of a collision can be described by the probability of two or more simultaneous arrivals. The delay due to a collision is determined by the time required to recognize contention, issue the jamming signal (approximately 1 microsecond), wait for the appropriate gap time, and then wait for the appropriate timeslot. Because the load distribution is assumed to be equal among the network BIUs, the average delay for the timeslot count to reach the assigned time is one-half the total scan time for the timeslot sequence as determined by the loading conditions.

Looking at the access delay encountered by a message under the ordered access mode, two conditions are possible: (1) message ready before the timeslot arrives, or (2) message ready after the appropriate timeslot has passed. For an equal load distribution, the probability of each case is 0.5.

- Transport Delay.
  - The transport service time is determined by the transmission rate, the message length, and the overhead required for each transmitted packet. The overhead includes the following:
  - Gap time between messages.
  - Turnon time.
  - Packet encapsulation.
  - Acknowledge turnon.
  - Propagation delay.
  - Acknowledge message.

System level fault management is further facilitated by the monitoring of network statistics at each node. During operation, the BIUs collect the following statistics:

- Number of collisions.
- Number of collisions during own transmission.
- Number of packet rejects due to decoder buffer full.
- Number of successful transmissions.
- Number of unsuccessful transmissions.
- Number of data transmissions received.
- Number of status responses received.
- Number of commands received.

### 4.3. Failure Modes and Effects

Operation of digital aircraft requires the proper function of a number of interconnected systems, subsystems, and components within the framework of an integrated bus structure. Intermittent or erratic behavior or total failure of one or more modules can impact the ability of the aircraft to perform its intended function. In some cases, the impact will be transparent as the fault is automatically detected, the failed module identified, and a redundant "like element" (similar or dissimilar) activated or "switched-to" automatically. Continued successive failures (or in the worst case, multiple simultaneous failures) could result in increased pilot workload, loss of function, or in the most severe case, the total loss of aircraft.

Because of the interactive relationships among systems and subsystems in aircraft, failures may propagate. Errors may affect not only the subsystem in which the failed module is embedded but also other subsystems to which erroneous data is transferred. This failure propagation potential between multiple systems/subsystems is greatly magnified by the differing levels of functional integration where data and information are exchanged between and among subsystems (using bus architectures and structures) as a requirement for normal operation.

Failures that could cause loss of essential mission capability or loss of aircraft must be protected against by using equipment redundancy, analytical redundancy, or functional redundancy to provide for continued operation after one or more failures. The redundancy may be applied at the system level (multiple buses or FCCs), at the sensor level (redundant Inertial Navigation System (INS), Altitude Heading Reference System (AHRS), Digital Air Data Computer (DADC), etc.), or at the module level (multiple similar or dissimilar microprocessors located in multiple processor subsystems). Failures that result only in some loss of function, restricted operation, or increased pilot workload, may or may not require redundancy. Redundancy requirements depend on the exact nature of the loss and the probability that such a loss will impact aircraft performance or aircraft flight safety. Failures that reduce the level of hardware redundancy or analytical redundancy, without loss of functional capability, may be able to be tolerated without performance degradation.

Failures can result from external disturbances or internal malfunction and can be either transient or permanent. Transient faults can often be ignored if the system is designed to tolerate such faults. In other cases, a transient fault can cause a more serious failure, such as the interruption of an instruction sequence in a computer, which in turn could cause a time-out or retry sequence, resulting in the completion of the computation using "stale" data. Permanent failures, on the other hand, must be recognized as such, and action must be taken to reconfigure around the failure.

Environmental effects can often be the cause of the failure. In the case of wire buses, heat, power supply surges (spikes), or low voltage levels could cause permanent or intermittent loss of an electronics unit or corruption of the bus data, which in turn would cause incorrect data and/or information to be passed to another unit in the hierarchy. Loss of electrical integrity (due to faulty shielding, grounding, or loss of cable integrity) could result in susceptibility to electromagnetic radiation, thus causing erroneous or erratic behavior.

In general, failures may exist in any one of the five functional elements relating to the integration of two or more subsystems. These functional elements include the following:

- Computers that process the data exchanged between subsystems.
- Data bus interfaces.
- Data bus(es).
- Input/output devices that govern the transmit/receive functions.
- System software.

Table 4.3-1 (McSharry, 1983) summarizes the potential faults which can cause intermittent or erratic behavior or even total failure of the networked architecture to communicate data and information to the various systems/subsystems within the structure.

The following considerations concerning the possible failures of digital data buses must be taken into account: First, transmission failures that may occur; second, effects on subsystems that are connected to the data bus by a bus controller or remote terminal failure; and third, effects of multiplex hardware failure. The navigation system must be self-contained and the aircraft must not become "lost" because of any type of transient. These safety requirements lead to subsystem requirements to store critical data in multiple locations and to recover rapidly from failures and upsets.

There are three failure modes, as follows: First, no transmission; second, incorrect transmission; and third, failure to relinquish control. A fault with these failure modes and some of the related causes are shown in figure 4.3-1.

## 4.4. Transmission Error

If the multiplex terminal hardware detects either an invalid word or a transmission discontinuity, the word and message are to be considered invalid. This message invalidation requirement may cause some systems (i.e., Electrical Multiplex (EMUX)) a problem. Since the EMUX systems usually have bit-oriented data rather than word or multiple word (message) oriented data, errors in a word following the reception of good data will invalidate good data.

Message completion failures should always be detected in a multiplex system. They are detected by the bus controller when the status word is suppressed or the message error flag in the status word is set. The message error flag removes ambiguity as to whether the error occurred before the message was validated by the remote terminal or in the response to the message.

Data transmission errors are handled by special error-handling interrupt software. The software will indicate whether (1) the command is to be retried, (2) the bus is to be used for the retry, and (3) the transmitted data (if any) should be invalidated. Tables 4.4-1 and 4.4-2 (MIL-STD-1553 Designer's Guide,

TABLE 4.3-1. DIGITAL DATA BUS SYSTEM FAILURE MODES AND EFFECTS (Adapted from McSharry, 1983)

| 1.0 COMPUTER FAULTS | 2.0 DATA BUS AND INTERFACE | 3.0 INPUT/OUTPUT | 4.0 SYSTEM REDUNDANCY/MANAGEMENT FAILURES |
|---|---|---|---|
| 1.1 Computer Hardware Faults | 2.1 Data Bus Hardware | 3.1 Input/Output Device | 4.1 Design Failure (Fault) |
| 1.1.1 Central Processor Unit (CPU) Failure | 2.1.1 Open/Short-Single Bus/Multiple Buses | 3.1.1 Hardware Failures | 4.1.1 Synchronization-Time Skews (Comparison Monitoring of Time Tag Data) |
| | | 3.1.1.1 Sensor, Sensor Output Transducer, Discrete Signal Input Failure | |
| 1.1.2 Memory Failure (Error) | 2.1.2 Interface Unit Failure | | 4.1.2 Generic Failure Modes - Power Interrupts, Software Design Faults, Common Mode Failures |
| 1.1.3 Discrete and Analog Input/Output Failure | 2.1.2.1 Failure to Respond | | |
| | | 3.1.1.2 Induction of Noise (or Other Oscillary Disturbance) Due to EMI/EMC | |
| | 2.1.2.2 Response to Wrong Address (Failure Diagnosis: Good = Defective) | | |
| 1.1.4 Clock Failure | | | |
| 1.2 Computer Software Failures (Faults) | | 3.1.2 Software Faults (Errors) | |
| | 2.1.3 Bus Controller Unit Failure - Site Selection Error | | |
| 1.2.1 Failure to Isolate Faulty Entity | | NOTE: Typical Failures Include: | |
| | 2.1.3.1 Multiple/Redundant Controller Selection - Hardware Arbitration | o Hardover to Max/Min Values<br>o Steady Zero Values<br>o Bias Offset<br>o Reduced Dynamic Response<br>o Sensitivity Change | |
| 1.2.2 Isolation of Good Component as Failed | | | |
| 1.2.3 Processing Erroneous Data | 2.1.3.2 Multiple/Redundant Controller Selection - Software Algorithm Fault (Error) | | |
| 1.2.4 Failure to Complete Task - Exceed Task Time Allocation | | | |
| 1.2.6 Observability | 2.1.3.3 Non-Centralized Controller Hardware Time-Out (Output Stage) Failure | | |
| | 2.1.4 Improper Decoding/Encoding of Address, Command, Data Word Structures | | |

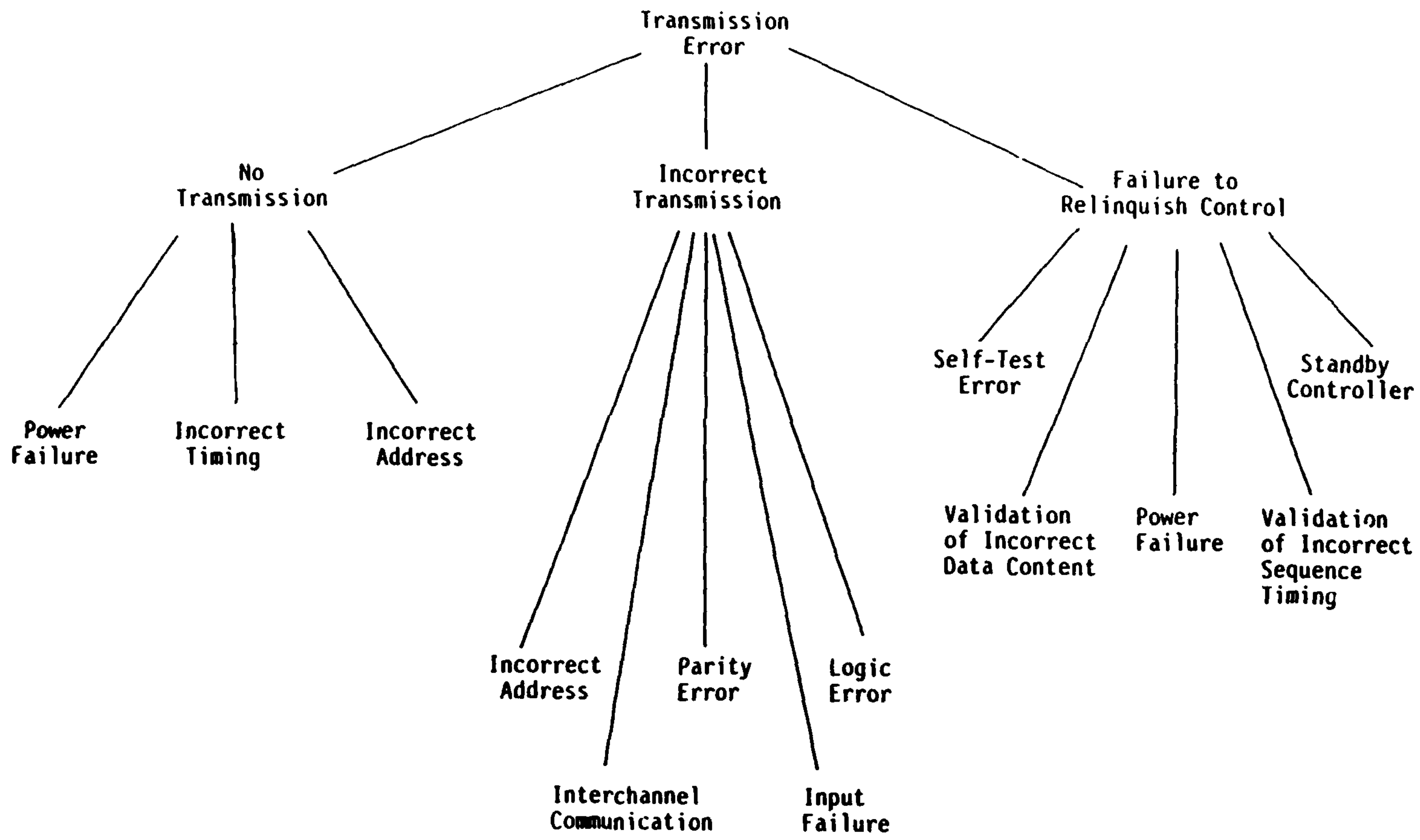


FIGURE 4.3-1. SIMPLE FAULT TREE EXAMPLE

TAB:⊦ 4.4-1. FAILURE CLASSES [MIL-STD-1553B]
(MIL-STD-1553 Designer's Guide, 1983)

| ERROR IDENTIFICATION | BUS SYSTEM | SENSOR |
|---|---|---|
| a. Message error | Transmission from bus controller to to terminal was decoded with error condition by receiving remote terminal | -- |
| b. Busy | Remote terminal unable to transmit or receive data at this time | Remote terminal and sensor unable to transmit or receive data at this time |
| c. Subsystem flag | -- | Sensor failure preventing proper sensor actions |
| d. Terminal flag | Remote terminal failure preventing complete action by terminal | Remote terminal portion of sensor interface has failure preventing complete action by terminal |
| e. Parity error (incorrect odd parity) | Error in status word; data not usable | Error in status word; data not usable |
| f. Improper sync | Unknown problem -- ignore; continue to look for valid sync | Unknown problem -- ignore; continue to look for valid sync |
| g. Invalid manchester | Error in message -- ignore data in message | -- |
| h. Improper number of data bits and parity | Error in message -- ignore data in message | -- |
| i. Discontinuity of data words | Error in message -- ignore data in message | -- |
| j. No status word response | Unknown problem -- requires further investigation | Unknown problem -- requires further investigation to achieve error |

TABLF 4.4-2. TYPICAL ERROR-CORRECTION TECHNIQUES [MIL-STD-1553B] (MIL-STD-1553 Designer's Guide, 1983)

| ERROR IDENTIFICATION TYPES | ERROR CORRECTION TECHNIQUE |
|---|---|
| 1. Bus system failures | |
| a. No status word response | Retry message on same bus n times |
| b. Message error | Retry messages on alternate bus n times |
| c. Parity error | Transmit status word mode code on each bus |
| d. Invalid Manchester | If necessary, transmit initiate self-mode code |
| e. Improper number of data bits and parity | Transmit BITE mode code |
| f. Discontinuity of data words | Analyze failure and determine corrective action, which may involve the following mode commands:<br>Shut down transmitter<br>Inhibit terminal flag bit<br>Transmit reset remote terminal mode code |
| g. Busy | Retry message on same bus after a fixed delay time |
| h. Terminal flag | If necessary, transmit initiate self-test mode code<br>Transmit BITE mode code<br>Analyze failure and determine corrective action, which may involve the following mode commands:<br>Shut down transmitter<br>Inhibit terminal flag bit<br>Transmit reset remote terminal mode code |
| i. Improper sync | Ignore and reset for valid sync |
| j. Subsystem flag | Retransmit the data (address/subaddress) to examine sensor BITE discretes or words |
| 2. Sensor failure | |
| a. Discretes<br>b. BITE data word(s) | Analyze failure and determine system-oriented corrective action |

1983) show the error identification types and the corresponding failure classes and error correction techniques.

- No Transmission. The user should listen to the bus it transmits on for its request address. If no bus controller activity is detected, the user should transfer listening to the other bus for its request address. If no activity is detected on the other bus, the user should continue toggling between the buses in search of bus controller activity.

- Incorrect Transmission. The most serious failure for the bus controller is erroneous transmission. An independent frequency source should be used by the bus controller to provide monitoring and detection of transmission frequency faults. The two common types of transmissions are broadcast (which is sent on all of the channels) and CR (which is sent to a specific address). An error in a broadcast transmission has the potential for system failure if it is incorrectly validated at each of the addresses. An error in a CR has a more limited effect since it only involves one address. Each receiver should incorporate isolation provisions to ensure that the occurrence of any reasonably probable internal LRU or bus receiver failure does not cause any input bus to operate outside of its specification limits (both under voltage or over voltage).

- Failure to Relinquish Control. Subsystem or terminal failures may be detected using Built-In Test (BIT) circuitry. These failures are reported by the setting of the subsystem flag bit or the terminal flag bit in the status word. In aircraft, dual-redundant buses are used, so a terminal failure may be isolated to one bus. Depending on the capability of the remote terminal hardware, the transmit BIT word mode code can be a powerful diagnostic aid. For each fault, the action to be taken must be determined, designed for, and implemented by the system.

Subsystem or terminal failures can also be detected without the use of the optional terminal or subsystem flags. Bad data or nonvarying data from a subsystem may be interpreted as a subsystem failure. Repeated message completion failures to a remote terminal via all possible data paths could be considered as a loss of the terminal function. The system software should be used to detect these failures.

Bus controller operation in the event of failure is important to an integrated data bus system. The primary bus controller should relinquish bus control whenever it suffers a power interruption that might cause erroneous outputs. The primary bus controller should detect its own bus control processing faults and remove itself as controller in a fail-passive manner. Similarly, the backup bus controller should recognize invalid control messages or the absence of valid control messages and revert to active bus controller status. Monitoring techniques should provide coverage for both hardware faults and software errors. Any undetected fault in the primary bus controller, which results in continuous erroneous transmission, will make all standby controllers ineffective. The bus controller is structured such that two independent faults must occur in order to cause erroneous transmissions.

## 4.5. Reliability for Flight Safety

Flight safety requirements allow no more than one unrecoverable failure in the flight control subsystem per $10^9$ flights. This failure rate is consistent with AC-25-13091 and is appropriate for integrated systems. The failure rate must encompass the entire flight control system including the necessary supportive electrical power, hydraulics, and any other subsystem used in the flight-critical capacity. When applied over the 2- and 3-hour mission duration of the aircraft, a maximum failure rate of approximately 5 x $10^{-6}$ failures per flight hour (for a 2-hour mission) and 3.3 x $10^{-6}$ failures per flight hour (for a 3-hour mission) can be allowed.

Figure 4.5-1 gives an example for the determination of the loss of bus control. The potential failures for the bus control example are given in table 4.5-1. The total failure rate must be equal to or less than the total allowable defined above. *In the example, the loss of bus control*, D, is

$$D = (E_1 + E_2 + E_3)(E_4 + E_5 + E_6) + E_7 + E_8 + E_9 + E_{10}$$

By substituting in the values from table 4.5-1, we obtain

$$D = 3.1012321 \times 10^{-5}$$

Therefore, in this example the data bus would fail to meet the reliability requirements for flight safety.

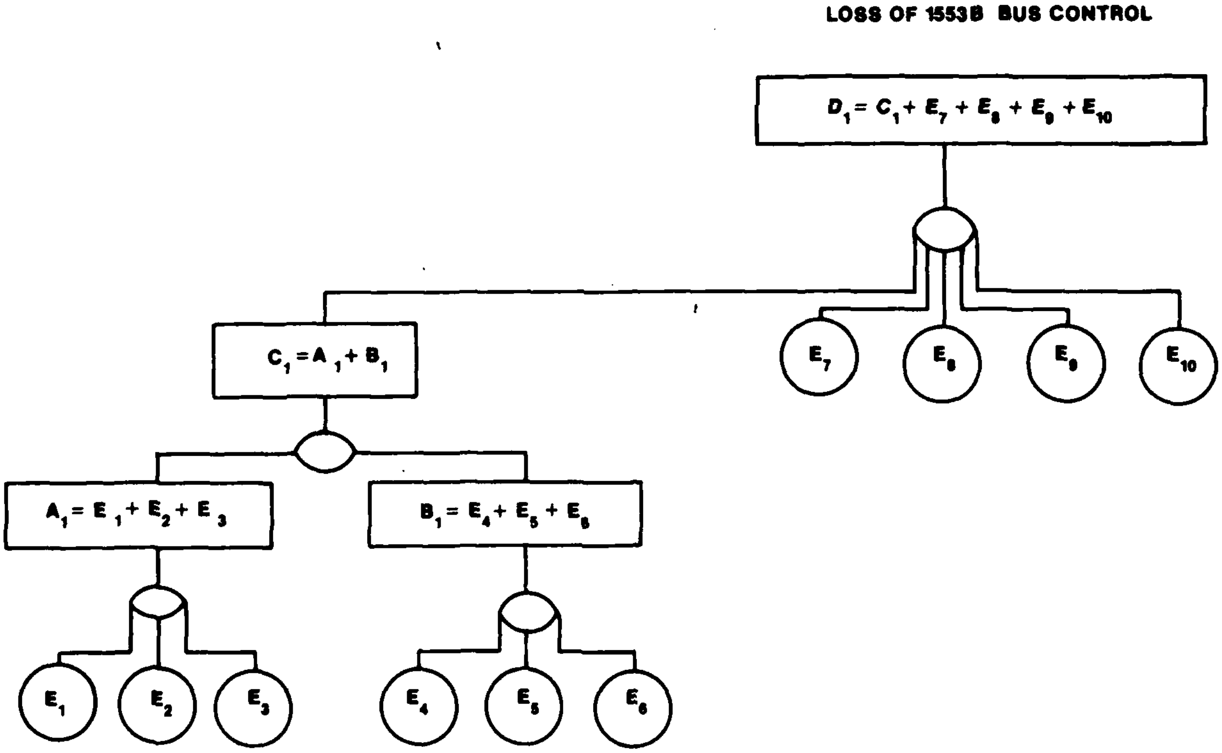


FIGURE 4.5-1. SINGLE CHANNEL-DUAL OUTPUT (BUSES A AND B) BUS CONTROL

TABLE 4.5-1. POTENTIAL FAILURES RESULTING IN LOSS OF BUS CONTROL SINGLE CHANNEL - DUAL OUTPUT (BUSES A AND B)

| ERROR | ERROR SOURCE | FAILURE RATE |
|---|---|---|
| $E_1$ | Bus A - Transformer Failure | $10^{-6}$ |
| $E_2$ | Bus A - Transceiver Failure | $10^{-4}$ |
| $E_3$ | Bus A - Decoder Failure | $10^{-5}$ |
| $E_4$ | Bus B - Transformer Failure | $10^{-6}$ |
| $E_5$ | Bus B - Transceiver Failure | $10^{-4}$ |
| $E_6$ | Bus B - Decoder Failure | $10^{-5}$ |
| $E_7$ | Single Encoder Failure | $10^{-5}$ |
| $E_8$ | Internal Control Logic Failure | $10^{-5}$ |
| $E_9$ | Interface Unit Failure | $10^{-5}$ |
| $E_{10}$ | Microprocessor System Failure | $10^{-6}$ |

# 5. FIBER OPTIC DATA BUS FOR AVIONICS INTEGRATION

## 5.1. Elements of Fiber Optic Data Bus

As stated in previous sections, the bus topology is the physical arrangement and interconnection of the various terminals. In a fiber optic bus, the elements utilized are optical couplers, fiber cable, connectors, and splices.

TABLE 5.1-1. OPTICAL BUS TECHNOLOGY LIMITS

| COMPONENT | FACTORS |
|---|---|
| Couplers | Losses<br>Number of Taps |
| Fiber | Fiber Type<br>Modal Noise<br>Connectors<br>Splicing<br>Reflections<br>Cabling |
| Optical Source | Power<br>Speed |
| Optical Receiver | Sensitivity<br>Intermessage Dynamic Range<br>Intermessage Response Time<br>Clock Recovery |
| Processing/Interface Logic | Speed<br>Power Consumption<br>VHSIC/VLSI & GaAs |
| Topologies | Performance<br>Reliability<br>Flexibility<br>Installation and Maintenance<br>Cost |

The design of these elements not only relates to system performance but also to system installation and maintenance. Because optical power losses occur whenever any of these components or functions are inserted in the optical path, performance is affected. Table 5.1-1 presents the components and factors that influence the limits of optical bus technology as it applies to buses used for avionics integration.

### 5.2. Optical Cables

Considerations involved in evaluating optical cables for a fiber optic data bus include fiber design (including modal noise and reflection effects) and cable type and construction.

### 5.3. Optical Path

Basically, the optical path is the fiber optic cable. In designing the proposed avionics architecture, the fiber cable must be selected for minimal loss (across the bus) and wide bandwidth. In addition, the fiber cable must be constructed for strength and endurance during the life of the bus architecture, ease of installation, and long term environmental performance.

### 5.4. Splices and Connectors

Interconnections between the fiber cable elements (controllers, remote terminals, junctions, etc.) can be made with either splices or connectors. Splices in the fiber cable are easier to incorporate and provide lower losses than connectors; however, splices are permanent. Connectors, on the other hand can be mated and unmated hundreds of times with virtually no degradation in performance. Therefore, in the development (and design) of a fiber optic based avionics architecture, optical couplers (connectors) should be utilized for bus interface connections to the physical bus. This will minimize downtime due to repair or change in the architectural structure when remote terminals are added or deleted. In the case of aircraft having pressurized bulkheads, several penetrations through these bulkheads may need to be made. At these penetrations, the fiber optic cable can be run straight through the bulkhead or an optical connector (coupler) can be used on each side of the bulkhead. The tradeoff, in this case, is between the ease of installation and rework using a connector (coupler) system or the lower loss and absence of reflections using a spliced or through cable.

### 5.5. Optical Couplers

The two basic types of optical coupling techniques that are considered for an optical data bus are star couplers and taps or tees.

In a transmissive star, N ports are designated as input ports, and N ports as output ports. The optical energy on any input port is split more or less equally among all output ports, with a splitting loss of 10 log N. Star couplers also have an insertion loss and a port-port variation of 1 to 3 Decibel (dB), each depending on the number of ports. Stars in excess of 100 ports have been fabricated; however, for minimal cost and port-port variations, the practical limit of current technology is 64 ports.

Directional couplers for tapping a transmitter and receiver onto a fiber optic bus are basically like a four-port transmissive star with an excess loss of 0.5 to 1 dB. Typically a tap into the receiver can be accomplished with a 90/10 or 95/5 split providing a 0.5 to 2.0 dB link throughput loss, respectively, and a 10 dB to 13 dB tap-off or reduction of the link power into the bus receiver. For tapping the transmitter into the bus, the throughput loss as well as the coupled transmitter power reduction is 3 dB in commercially available couplers.

## 5.6. Size

Of the available fiber options, the 100/140 micrometer (μm) or the 85/125 μm graded index fiber operating at a 0.05 μm signal length is optimum because:

- Their large core, high numerical aperture, and operation wavelength support many more modes, thus minimizing the modal noise limitation.

- Their large core enables greater Light Emitting Diode (LED) coupled power, thus extending the application of LEDs.

- Their core-clad geometry makes it easier to make low excess loss star couplers.

## 5.7. Reflections

Another consideration in the medium analysis is reflections. Reflections result from an index of refraction discontinuity at connectors, poor splices, or mismatched fiber types. For example, with a star coupler, the main signal passes through the link; however, part of the signal is first reflected at the star coupler dry connector (8 percent) and then again at the transmitter dry connector (8 percent). The resulting reflected signal is down 22 dB with respect to the main signal and delayed by as much as 1 microsecond (1 ns/m). This reflected signal becomes a problem if it overlaps the next bus transmission and shows up as noise superimposed on this data. Therefore, consideration must be given to minimize reflections.

## 5.8. Connectors

Optical connectors, which are suitable for use in a data bus, are low cost, easily installed, and typically low loss. The connector loss depends on the fiber size as well as the quality of the connector. For 100/140 μm fiber, losses vary from 0.5 to 1.5 dB depending on connector quality. Available multiway connectors have the advantage of simplifying a bulkhead penetration and provide quicker connect/disconnect of a multifiber cable. Although there is no fundamental reason for higher loss in a multiway connector, the losses in currently available connectors average approximately 0.5 to 1 dB more than the loss in a single fiber connector.

## 5.9. Splicing

For field installation, maintenance, and repair the elastomeric splicing system has been identified as the best currently available splicing technique.

## 5.10. Technology - Optical Bus Transmitters and Receivers

Fiber optic bus Transmitter/Receiver (T/R) design is driven by the goal of maximizing bus efficiency. This is necessary to fully utilize the benefits of the bus, minimizing "dead" time, and allowing transfer of significant quantities of data.

An efficient bus T/R is relatively easy to design. However, providing very quick transmitter power output stabilization and very short receiver settling time at the start of a message significantly increases the difficulty and complexity of the T/R design. A fast response clock recovery scheme is also critical in minimizing the amount of time used for non-data. In summary, the more time that is used to perform overhead functions, the less time there is to transmit data, and the lower the efficiency of the bus.

## 5.11. Maximizing Bus Efficiency

One of the principal considerations in maximizing bus efficiency revolves around the unique aspects of an optical transmission. Intensity modulation of an optical carrier provides a unipolar transmission channel, unlike electrical current transmission over wire which may be bipolar. Unipolar signaling causes a Direct Current (dc) shift between signal-on, and signal-off states, which will disturb the operation of conventional receiver amplifiers having ac coupling until the interstage coupling capacitances have had time to accommodate the shift. A similar dc shift occurs between small and large signals.

Thus to avoid a long settling time at the start of messages, receivers designed for data bus application either have a short ac coupling time constant to minimize the disturbance time, or employ dc coupling. If dc coupling is used, more complex circuitry is required for setting the data decision threshold for the received waveform. The shift in average power between signal and no-signal states also complicates laser optical source power stabilization, which is normally accomplished using average power feedback control.

## 5.12. Transmission Losses

Optical bus configurations have considerable and somewhat undefined transmission losses between source and detector, resulting from the couplers and connectors. When combined with source power and detector sensitivity variations, this gives rise to an uncertain received power level. A high-gain, wide-dynamic-range receiver is required. Since time is a premium, long term averaging is undesirable. Alternate methods for rapidly accommodating the dynamic range are required. This is a major concern for optical data bus receiver designers.

## 5.13. Receiver Losses

Three receiver types which provide simple, instantaneous adjustment to message levels are known. In the symmetrical clamp receiver, all signals are bit-by-bit clamped to the same low level. After amplification, decisions about the validity of data are based on the data being above a fixed threshold. Good dynamic range is achievable and start-of-message time constant delays are eliminated. This is not the case with conventional linear or limiting receivers. The technique operates well up to bit rates around 50 Million bits per second (Mbps). Above this level implementation problems arise. (The upper bit rate limit may be extended using lower capacitance hybrid construction.) This technique is a leading candidate for receivers operating at lower data rates.

A second fast response scheme uses a dc coupled receiver (to avoid ac coupling time constants) and a bit-by-bit adaptive threshold decision. The technique is ideally suited to very high data rate reception but dynamic range is limited by amplifier design. Optimum performance is limited by dc offset in the amplifier, which may be a limitation for wide temperature range operation.

High-bit rate reception may also be handled efficiently with a high-pass filtering receiver when the signal is any biphase code or other reduced low-frequency content code. This is because required coupling capacity time constants become small compared to the fixed bus intermessage dead time resulting from propagation delays. Appropriate filters have been designed with a linear phase response in the stop band, providing an intermessage response time as low as six bit times for Manchester coded data.

Conventional point-to-point system optical receivers have well defined sensitivity limits that may be calculated from the thermal and shot noise of the devices. For data bus receivers, a number of compromises in design are necessary to achieve fast response to messages. These generally result in less sensitivity. Similarly, wider dynamic range may generally be achieved in a receiver, which has a long period to adjust to changes in signal level, versus a receiver that is required to adjust almost instantaneously.

The receiver sensitivity is affected largely by the type of photodetector and by preamplifier design. A silicon avalanche photodetector offers greatest sensitivity (at 0.85 $\mu$m); therefore, preamplifier design is less critical. At 0.85 $\mu$m, a silicon PIN diode with a sensitive preamplifier has approximately 10 dB less sensitivity.

## 5.14. Transmitter Losses

For relatively low rate transmission, i.e., <10-50 Mbps, little difficulty exists in designing a transmitter circuit using LEDs. Data modulation may be dc coupled through to the LED and any data format or message length may be accommodated. Very high data rate transmission requires the use of a semiconductor laser diode to achieve the required modulation rate and sufficient launched optical power to provide reliable reception after the transmission losses. Lasers require a more complex driver circuit to ensure that the drive current compensates for temperature and aging of the source, and is correctly prebiased during transmission to avoid data distortion resulting from lasing turnon delay. Effective compensation of the drive current requires feedback control of the launched signal. Feedback control commonly operates by stabilizing the average transmitted power in continuous transmission point-to-point systems. With the burst nature of transmission in a bus system, averaging is not as convenient and requires a long preamble for the laser power to initially stabilize.

Any data bus transmitter design must include an override control, which provides a positive curtailment of transmission in the event of a nonself-correcting fault. An external timeout circuit or protocol function controls this override function.

## 5.15. Optical T/R Power Margin

A key element in the design and optimization of any fiber optic link including a data bus is the system power budget analysis. Such an analysis is important not only to ensure that there is adequate optical power at any given receiver under all conditions, but also to ensure, particularly in a data bus, that there is not too much optical power at any given receiver.

There are three basic elements to a power budget analysis: system losses, optical source output power, and optical receiver sensitivity. The maximum allowable system loss can be derived for a transmitter combined with a realizable receiver. Output powers of -6 Decibels per meter (dBm) can be achieved with high radiance LEDs coupled to 100 $\mu$m core fiber with an Numerical Acceptance (NA) of 0.3.

## 5.16. Topology Analysis

Using the practical technical limits as discussed in the previous sections, an analysis of various fiber optic data bus topologies or configurations was performed to evaluate the number of terminals possible at various data rates.

The topologies examined included:

- Linear.

  Inbound-outbound (loop or ring).
  Bidirectional (open-ended).
  Active.

- Star.

  Transmissive.
  Reflective.
  Star-star.
  Active star-star.

- Hybrids.

  Star-loop.
  Loop-star.

Since active stars and active rings are essentially point-to-point links, bus losses are not the limiting factor on the number of terminals, nor is dynamic range a factor in receiver design.

For this initial, first-order analysis, the best case performance for splices, connectors, and couplers was assumed. This approach "brackets" the problem by defining the best possible performance of a particular topology implemented with currently available (or nearly available) technology.

A passive transmissive star bus is the most efficient topology, because the power from any transmitter is distributed evenly among all receivers. In addition, there is only one coupler-insertion loss between any given T/R pair.

The principal disadvantage of a bus with a single star is that the cables from all T/R modules must be run to the star. In an aircraft, this increases the initial installation cost due to the increased number of bulkhead penetrations required. In addition, there is little flexibility for adding new terminals at arbitrary locations. One solution to this is to provide a distributed bus topology such as a star-star or a star-linear topology. The performance of the star-star topology can be easily improved by adding a single repeater (or two for redundancy) at the central star.

Two hybrid topologies combining stars with a linear bus concept were investigated because they provided four separate nodes with the potential for improved performance over a simple linear bus. The first is a star-loop; the second a loop-star.

Initial analysis of these revealed very little reduction in bus loss over a simple linear loop, and therefore a detailed analysis was not performed. The loop-star or distributed star topology can be effective, however, with active repeaters between the stars.

The only viable passive topology for 128 terminals is a star; however, an active linear bus, active star, or active star-star are viable implementations for 128 terminals at 300 Mbps. The active star-star appears optimal because it:

- Minimizes cabling and bulkhead penetrations with four (or more) nodes for concentrated location of terminals while enhancing flexibility.

- Minimizes number of repeaters and therefore cost and maintenance.

- Prevents a single point failure that will disable the entire bus.

- Allows use of star couplers with 6-32 ports, reducing the cost and increasing the performance and reliability of the couplers.

## 5.17. Fiber Optic Network Based Losses

A typical set of requirements for an avionics multiplexed bus of a commercial transport could include anywhere from 32 to 128 terminals. Data rates could be in the 10-100 MHz (or Mbps) range. The bus probably would be bidirectional, using a broadcast type mode in which any terminal might transmit data to any other terminal in the network. Various topologies for such a bus have been discussed earlier; however, the most probable topology for such an architecture would be a star-coupled topology due to the fact that it can be implemented without the use of active repeaters. This results in higher reliability, lower maintenance, and reduced losses in the optical path.

Table 5.17-1 presents a typical loss budget calculated for an approximately 60-terminal, star-coupled transmission network. From this table, it can be seen that the bus network will require high optical output from the transmitter and high receiver sensitivity to assure that the integrity of the data is maximized. To insure the high integrity, the bus optical components will have to be selected to be consistent with simple straightforward system design at both the transmitter and receiver ends.

TABLE 5.17-1. STAR-COUPLED NETWORK LOSSES

| COMPONENT | MINIMUM LOSS | MAXIMUM LOSS | COMMENT |
|---|---|---|---|
| Fiber | 0.0 dB | 1.0 dB | 50 m. terminal to star maximum, 5 dB/km |
| Connectors | 0.4 dB | 8.0 dB | .1 dB to 1.0 dB each, 4 to 8 total terminal to terminal |
| Star Coupler | 17.1 dB | 21.1 dB | Typical |
| TOTAL | 17.5 dB | 30.1 dB | |
| | Optical Dynamic Range: 12.6 dB | | |

# APPENDIX A - MODULATION AND SIGNALING METHODS

Modulation changes the carrier signal's characteristics. An unmodulated carrier is a periodic signal containing no information. Modulation imposes information on the carrier. Analog carriers can be represented by the sine wave:

$$a = A \sin (2\pi f t + \phi)$$

where

$a$ = voltage at time $t$<br>
$A$ = maximum amplitude<br>
$f$ = frequency<br>
$\phi$ = phase

The carrier's amplitude, frequency, and phase can all be modified. Amplitude Modulation (AM) refers to modification of the carrier's amplitude for information transfer. Frequency Modulation (FM) refers to modification of the carrier's frequency. Phase modulation ($\phi$M) refers to modification of the carrier's phase.

- Frequency Modulation.

  FM is not commonly applied to information transfer in digital avionics systems.

- Amplitude Modulation.

  The simplest form of AM varies the magnitude of the signal (A) from zero to a fixed peak-to-peak voltage. The zero level represents a binary zero and the maximum voltage represents a binary one. Figure A-1 (Held, 1986) shows the correspondence between the AM signal and the digital data it represents. AM by itself is normally used for very low data rates. For higher transmission rates, AM may be combined with $\phi$M.

- Phase Modulation.

  $\phi$M varies the phase of the carrier signal. Figure A-2 shows an example of $\phi$M.

In terms of bus transmission of digital data, modulation techniques and signaling methods refer to the type of coding used to transmit information through the bus. All of the subsystems connected to the bus must use the same coding method. There are a number of codes that can be used, which differ with respect to advantages and disadvantages. This brief section of the tutorial looks at the coding methods likely to be used by aviation-oriented data buses.

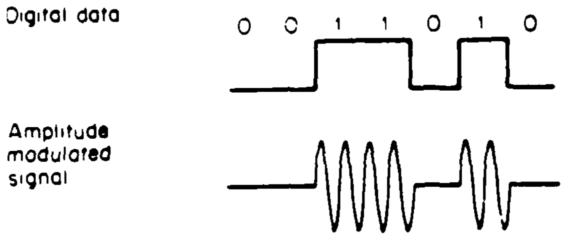


FIGURE A-1. AMPLITUDE MODULATION
(Held, 1986)

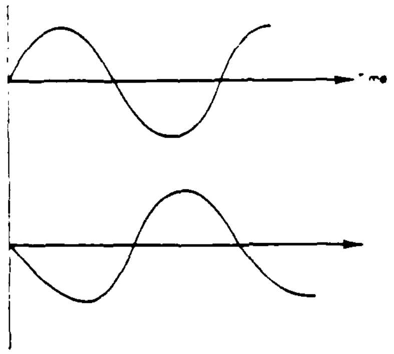


FIGURE A-2. PHASE MODULATION

Code is categorized as either single-density or double-density. Double-density codes include Delay Modulation (DM), Modified-Frequency Modulation (MFM), Group Code Recording (GCR), Zero Modulation (ZM), Enhanced Non-return to Zero (ENRZ), and Randomized Non-return to Zero (RNRZ), most of which are not appropriate for aircraft data buses. An exception is DM coding.

DM coding is complex both in hardware and functional characteristics. Its functional complexity stems from the requirement that there must be at least one signal transition for every two-bit interval and no more than one transition per bit. Because of this, some synchronization capability is still provided, but at a lower modulation and bandwidth requirement than required for the single-density codes. Consequently, it cannot be used effectively with buses requiring high data transfer rates.

The most common single-density codes are Non-return to Zero (NRZ); NRZ-Inverted (NRZ-I), which is sometimes referred to as NRZ-M; NRZ-Dual Level (NRZ-L) ratio; and biphase. Biphase covers several subcategories: Manchester II, FM, and Phase Encoding (PE). Since these single-density codes are self-clocking, the clock is represented by level transitions, which take place even if data transitions do not. NRZ, Return to Zero (RZ), and biphase are categorized by the suffixes L (level), M (mark), and S (space). An -L suffix indicates that data are represented by different levels; -M and -S suffixes indicate that data are represented by the presence or absence of transitions. In codes designated -M, a "1" (defined as a mark) occurs with a level transition; "0" is no transition. The converse is true for codes designated -S.

NRZ codes remain constant throughout a bit interval and either use absolute values of the signal elements or differential encoding where the polarity of adjacent elements is compared to determine the bit value. This method lacks independent synchronization and error-detection capabilities but provides efficient usage of the bandwidth.

RZ codes return to a binary "0" level at one-half the bit interval for binary "1" signals, requiring a higher bandwidth for an equivalent NRZ data rate.

Biphase codes include the Manchester and Differential Manchester techniques. At least one signal transition is required every bit interval, providing a self-clocking mechanism. The absence of the expected transitions may also be used for error detection. With two possible transitions per bit time, there is a corresponding increase in the bandwidth required.

Multilevel binary encoding schemes use more than two signal levels. One method is bipolar, which has no synchronization capability but does provide some error detection by requiring successive binary "1"s to be of opposite polarity.

Most of the aircraft data buses use biphase codes like Manchester II, which is self-clocking since the data and clock are included in a single serial data stream. In clocked systems, the clock defines the size of the data-bit cell; however, in nonself-clocking systems, speed fluctuations cause the data track to vary relative to the speed of the clock. Over a period of time, the clock will appear to speed up or slow down and will improperly define a data bit cell.

With self-clocking, everything stays synchronized. The mid-bit transitions of Manchester code help detect transmission errors.

Table A-1 summarizes the major features for some of the popular single and double-density codes. The encoded waveforms in figure A-3 illustrate patterns for an identical binary input produced by each form of encoding.

TABLE A-1. IMPORTANT PARAMETERS OF ENCODING TECHNIQUES

| | | | | | | Band | Preamble |
|---|---|---|---|---|---|---|---|
| | Bandwidth | | Storage | Self- | dc | Speed | for Synch- |
| Code | $f_l$ | $f_h$ | Efficiency | Clocking | Presence | Ratio | ronization |
| NRZ | 0 | 0.5f* | N.A. | No | Yes | N.A. | No |
| RZ | 0.25f | 1.0f | 50% | No | Yes | 4 | Yes |
| NRZ-S | 0 | 0.5f | 80% | No | No | 9 | No |
| Ratio | 0.75f | 1.5f | 33% | Yes | No | 2 | No |
| Biphase | 0.5f | 1.0f | 100% | No | Yes | 2 | Yes |
| Double-density | N.A. | 0.5f | 100% | No | Yes | 2 | Yes |

*Bandwidth in terms of the fundamental frequency of the data rate.
N.A. = Information Not Available

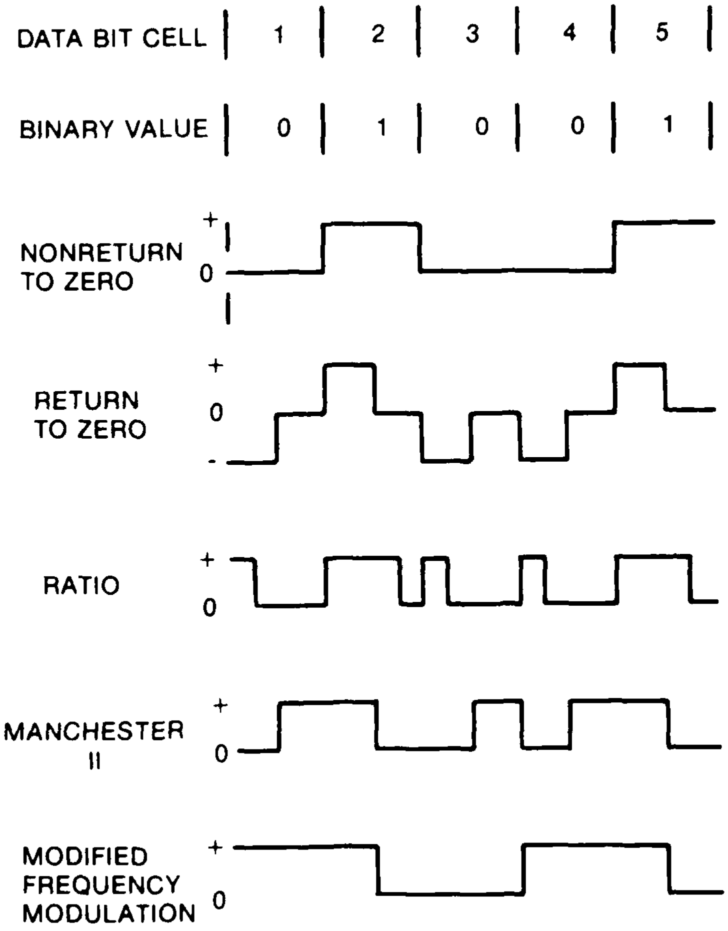


FIGURE A-3. WAVEFORMS GENERATED BY FIVE DIFFERENT ENCODING SCHEMES FOR A FIXED BINARY SIGNAL

# BIBLIOGRAPHY

ARINC Specification 429-5, Mark 33 Digital Information Transfer System, April, 1981.

ARINC Specification 629 (Multi-Transmitter Data Bus), Part 1 - Protocol Description and Part 2 - Label and Word String Definitions, Drafts dated September 1987.

Aydin Vector. MIL-STD-1553: Theory and Application, 2/84-2M, Newtown, PA, 1984.

Eldredge, D., and E. F. Hitt, Digital System Bus Integrity, FAA Technical Report, DOT/FAA/CT-86/44, Atlantic City Airport, New Jersey, March 1987.

General Aviation Manufacturers Association Specification, Washington, DC, February 1986.

Held, G. Data Communications Networking Devices. John Wiley, New York, 1986.

ILC Data Device Corporation. MIL-STD-1553 Designer's Guide, New York, 1983.

Jennings, R. G. "Avionics Standard Communications Bus: Its Implementation and Usage," Proceedings of the AIAA/IEEE Seventh Digital Avionics Systems Conference, Fort Worth, Texas, October 1986.

Kiernan, J. J., and J. R. Sims, "Standardization in Military System Architecture," Standardization in Military Avionics Systems Architecture, Proceedings of an IEEE/AES-S Seminar, Dayton, Ohio, November 28, 1979.

MIL-STD-1553B, Aircraft Internal Time Division Command/Response Multiplex Data Bus, Specification, 1978.

McSharry, M. E. Architecture Tradeoffs for Bus-Integrated Control Systems, NADC-82041-60, Aircraft and Crew Systems Technology Directorate, Naval Air Development Center, Warminster, PA, October, 1983.

Rich, B. A., et al., Multibus Avionic Architecture Design Study (MAADS), AFWAL-TR-83-1141, AFWAL, Wright-Patterson Air Force Base, OH, October 1983.

Society of Automotive Engineers, SAE High-Speed Ring Bus Standard, (Draft) March, 1987.

SAE Linear Token Passing Bus Standard, (Draft) April, 1987.

Schmitter, E. J., and P. Baues, "The Basic Fault-Tolerant System," IEEE Micro, 1984.

SCI Systems, Inc. *The MIL-STD-1553 Multiplex Applications Handbook*, Huntsville, AL, February 1982.

Shaw, J. L., H. K. Herzog, and K. Okubo, "Digital Autonomous Terminal Access Communication," *Proceedings of the AIAA/IEEE Seventh Digital Avionics Systems Conference*, Fort Worth, Texas, October 1986.

*Integrated Application of Active Controls (IAAC) Technology to an Advanced Subsonic Transport Project - ACT/CONTROL/GUIDANCE SYSTEM STUDY - VOLUME I. Final Report*, NASA Contractor Report 165963, NASA Langley Research Center, Hampton, VA, December 1982.

## GLOSSARY

ADDRESSING CAPACITY. The number of components addressable by the protocol used on a given data bus.

ASYNCHRONOUS MESSAGES. Electronic signals with transmission times that are not known a priori. These may include priority signals requiring immediate access to the bus.

BIT TIME. The time it would take to transmit one bit. Usually this is "blank" time when nothing is being transmitted. One nth of the bus speed (i.e., on a 1 kHz bus, the bit time is $10^{-3}$ seconds).

BLOCK TRANSFER. A data transfer mode allowing the transfer of variable length data blocks.

BROADCAST CAPABILITY. The capacity to transmit messages to all terminals simultaneously.

CAT IIIa LANDING. One of several landing categories defined in FAR 91. CAT IIIa implies the need for an instrument landing approach.

CENTRAL CONTROL. Control from one master, whether stationary or non-stationary.

COMMAND/RESPONSE. "Operation of a data bus system such that remote terminals receive and transmit data only when commanded to do so by the controller." (MIL-STD-1553 Designer's Guide, 1983, p. II-3).

CONTENT ADDRESSING. The system of identifying message recipients based on information embedded in the message. This is in contrast to destination terminal addresses.

DATA BUS. A system for transferring data between discrete pieces of equipment in the same complex.

DATA LATENCY. The delay from the time when a piece of information becomes available at a source terminal to the time it is received at the destination.

DATA LINK ASSURANCE OF RECEIPT. The guarantee of good data through the data link level.

DETERMINISTIC. A system where all parameters are known, as opposed to a statistical system where the outcome is subject to the laws of probability.

DISTRIBUTED CONTROL. Concurrent control from multiple points in the data bus system.

FAULT CONTAINMENT. The capacity of a system to prohibit errors and/or failures from propagating from the source throughout the system.

FAULT DETECTION. The capacity of a system to determine the occurrence of erroneous operation.

FAULT ISOLATION. The capacity of a system to isolate a failure to the required level so it can reconfigure.

FAULT TOLERANCE. The capability to endure errors and/or failures without causing total system failure.

INITIALIZATION. Setting the beginning parameters and values on system power-up. For redundant systems this includes setting the initial configuration of the system.

LABELED ADDRESSING. The system of identifying message recipients based on labels. This is in contrast to destination terminal addresses.

MESSAGE STRUCTURE. The organization of both protocol and data information in a message.

MONITORABILITY. The capacity of the protocol to be viewed passively to allow observation of the dynamics of the protocol.

NETWORK CONTROL STRATEGY. The solution proposed by the designer in addressing his specific problem (design flexibility).

NUMERICAL APERTURE. The angle of acceptance of light from a light source for a given fiber optic cable.

PARAMETERIZATION CAPABILITY. A measure of how well the attributes of the protocol can be described by parameters.

RECONFIGURATION. The capacity of a system to rearrange or reconnect the system elements or functions.

SYNCHRONOUS MESSAGES. Messages transmitted at a known a priori sequence and time or time interval.

SYSTEM INTEGRITY. The degree to which a system is dependable.

TESTABILITY. A measure of how well the protocol supports completeness of testing and the protocol's ability to produce repeatable or predictable results.

THROUGHPUT. The productivity of a data processing system as expressed in computing work per minute or hour.

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ac | Alternating Current |
| AE | Avionics Equipment |
| AES-S | Aerospace and Electronic Systems Society |
| AFWAL | Air Force Wright Aeronautical Laboratory |
| AHRS | Attitude Heading Reference System |
| AIAA | American Institute for Aeronautics and Astronautics |
| AM | Amplitude Modulation |
| ARINC | Aeronautical Radio, Incorporated |
| ASCB | Avionics Standard Communications Bus |
| BIR | Benchmark Information Rate |
| BIT | Built-In Test |
| BITE | Built-In Test Equipment |
| BIU | Bus Interface Unit |
| bps | Bits Per Second |
| CCITT | Consultative Committee for International Telephone and Telegraph |
| CD | Collision Detection |
| CR | Command Response |
| CRC | Cyclic Redundancy Check |
| CSMA | Carrier Sense Multiple Access |
| CSMA/CD | Carrier Sense Multiple Access/Collision Detection |
| CT | Technical Center (designation used in FAA report numbering scheme) |
| DADC | Digital Air Data Computer |
| DATAC | Digital Autonomous Terminal Access Communication |
| dB | Decibel |
| dBm | Decibels per meter |
| dc | Direct Current |
| DITS | Digital Information Transfer System |
| DM | Delay Modulation |
| DMA | Direct Memory Access |
| DOT | Department of Transportation |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| EMUX | Electrical Multiplex |
| ENRZ | Enhanced Non-return to Zero |
| FAA | Federal Aviation Administration |
| FADEC | Full Authority Digital Engine Controller |
| FAR | Federal Acquisition Regulation |
| FCC | Flight Control Computer |
| FM | Frequency Modulation |
| GaAs | Gallium Arsenide |
| GAMA | General Aviation Manufacturers' Association |
| GCR | Group Code Recording |
| HDLC | High-Level Data Link Control |
| HSRB | High-Speed Ring Bus |

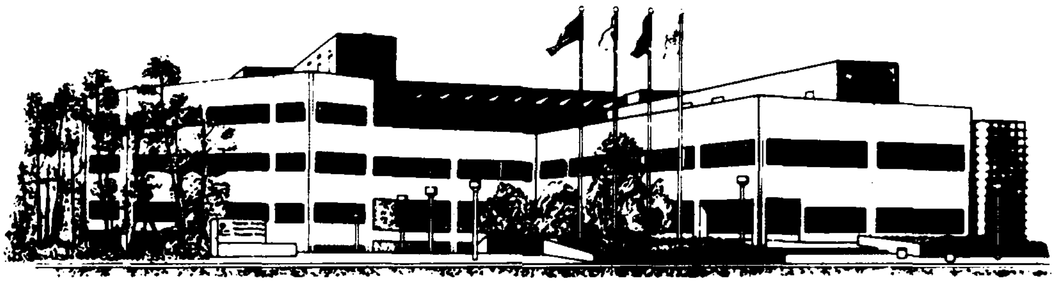
| | |
|---|---|
| IEEE | The Institute for Electrical and Electronics Engineers, Incorporated |
| INS | Inertial Navigation System |
| K | Thousand |
| KHz | Kilohertz (kilocycles per second) |
| km | kilometer |
| LED | Light Emitting Diode |
| LRC | Longitudinal Redundancy Check |
| LRU | Line Replaceable Unit |
| LSB | Least Significant Bit |
| LTPB | Linear Token Passing Bus |
| m | meter |
| μm | Micrometer |
| M | Million |
| MAADS | Multibus Avionic Architecture Design Study |
| Mbps | Million bits per second |
| MDT | Mean Down Time |
| MFM | Modified-Frequency Modulation |
| MHz | Megahertz |
| MIL-STD | Military Standard |
| ms | Millisecond |
| MSB | Most Significant Bit |
| MTBCF | Mean Time Between Critical Failures |
| MTTR | Mean Time To Repair |
| NA | Numerical Acceptance |
| NADC | Naval Air Development Center |
| NAECON | National Aerospace & Electronics Conference |
| NRZ | Non-return to Zero |
| NRZ-I | Non-return to Zero Inverted |
| NRZ-L | Non-return to Zero Dual Level |
| nsec | Nanosecond |
| PAS | Pilot Assist System |
| PE | Phase Encoding |
| ϕM | Phase Modulation |
| RAT | Ring Admittance Timer |
| RNRZ | Randomized Non-return to Zero |
| RZ | Return to Zero |
| SAE | Society of Automotive Engineers |
| str | string |
| TDM | Time Division Multiplex |
| THT | Token-Holding Timer |
| T/R | Transmitter/Receiver |
| VHSIC | Very High-Speed Integrated Circuits |
| VLSI | Very Large Scale Integration |
| VLSIC | Very Large Scale Integrated Circuits |
| VRC | Vertical Redundancy Check |
| ZM | Zero Modulation |

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II DIGITAL SYSTEMS VALIDATION

## CHAPTER 7
## ANALYTICAL SENSOR REDUNDANCY



**PREPARED BY:**

**COMPUTER RESOURCE MANAGEMENT, INC.**
**950 HERNDON PARKWAY, SUITE 360**
**HERNDON, VIRGINIA 22070**

**PREPARED FOR:**

**FEDERAL AVIATION ADMINISTRATION**
**TECHNICAL CENTER**
**ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405**

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

# 1. INTRODUCTION

The advent of modern digital controls has greatly changed the control technology and hardware implementation of aircraft flight control. These Digital Flight Control Systems (DFCS) provide enhanced performance for stability and control augmentation over an extremely wide range of flight envelope parameters. They also offer improved capabilities to operate in differing aircraft configurations from takeoff with wheels and flaps down to a high speed clean configuration with low drag, thrust, and low g forces. In addition to the performance enhancements in Digital Flight Control (DFC), the DFC computer has the capability to perform other computations to effect improvements in reliability and fault tolerance. Elaboration of these later features is the major thrust of this portion of the handbook.

The DFC improves reliability due to two factors. The first is the increased reliability of digital computer hardware relative to older technology; this enhancement leads to tens of thousands of hours between failures. The second factor is the increased reliability of the sensors and actuators which leads to several hundreds of hours between failures. The principal factor affecting DFC system reliability is reliability of the sensors and actuators.

The overall reliability required in today's flight control systems dictates the need for $10^{-9}$ probability of failure in cases where stability augmentation is needed for safe flight. This requires an increase in the reliability of the DFC components. The reliability of DFC computers may be achieved by utilizing dual processors, error detection, and fault tolerant designs. An increase in reliability of sensors and actuators may be achieved by means of redundant elements (dual or triple).

Assessment of this situation leads to a conclusion that redundant actuators and linkages are an adequate solution for actuation, and that DFC computers are adequate. The term Analytical Redundancy (AR) refers to the scheme for increasing the reliability of sensors by using the DFC computer for Fault Detection (FD) and isolation and for analytically determining estimates of sensor values.

Reliable DFC systems are burdened with large numbers of sensors which are required for both quality and redundancy. The demand for control quality has expanded the types of sensors used in basic augmentation functions. The yaw damper currently requires sensor data concerning attitude, angle of attack, and airspeed. The pitch damper requires a complex multifunction control law along with data from several sensors to drive multiple surfaces. The complexity of the sensors has improved quality; however, designs that meet overall flight control system reliability requirements lead to triple and quadruple replication of system components.

High levels of fault tolerance are mandatory for flight-critical control systems. Current Fly-By-Wire (FBW) systems utilize redundant computers, actuators, and sensors to achieve the necessary fault tolerance. Fault isolation (FI) is determined by some type of comparison or voting between like sensors. A one out of two sensor failure cannot be isolated by comparison techniques. In order to improve the reliability of a redundant set of sensors, one or more of the following must be implemented: increase the reliability of the existing sensors; add additional like sensors; synthesize the needed information; or isolate the remaining sensor if a failure occurs at the duplex level.

A large amount of sensor hardware is costly from a system standpoint. Sensors may act as antennas to increase electromagnetic susceptibility. The overall aircraft design may be constrained due to a large number of sensors. Therefore, there is a strong motivation to reduce the number of sensors. Significant reductions appear to be possible through a variety of methods. Recognized techniques for sensor reduction are control law modification and fault tolerant design. These methods may be used in combinations to optimize the number of sensors necessary for a particular application.

### 1.1. Control Law Modification

Control law modification ensures that operational requirements can be met with the minimum number of sensors and a better control system design. The control laws are modified to optimize the use of sensed data utilizing the analytical relationships which exist between sensors. The flight controller uses fewer sensed values in the basic single channel control laws, yet maintains the same performance as the controller which utilized all the sensor data. These modifications are application dependent.

Signal synthesis is one example of control law modification. The number of sensors required is reduced by synthesizing a signal or group of signals from a reduced set. The elements used to perform the synthesis are Kalman filters or Luenberger observers. Reduction in the number of sensors is a trade-otf against increased complexity of the control laws; this is a critical factor for analog systems. The trade-off in digital systems occurs in system performance. The bandwidth and noise content of the synthesized signal must be equivalent to the sensor eliminated. These techniques must be applied with care because of potential physical limitations which cannot be practically overcome.

Integrated flight management is another example of control law modification. This method works on the principle that subsystems which use common sensor types are combined. An example is the combination of the navigator and the flight control. The signal quality derived from the navigator is high and the data could easily be used by the flight control. Issues here are cost (since the navigator is normally not flight critical) and multiple failures.

### 1.2. Fault Tolerant Design

The following fault tolerant design techniques exist to meet reliability requirements using a minimum number of sensors. These techniques use fewer sensors to achieve the same level of redundancy as a quad-redundant system.

- Skewed and spec'al sensors.

- Sensor integratior.

- In-line sensor monitoring.

- Analytical sensor redundancy.

A skewed sensor arrangement significantly reduces the number of sensors required for Redundancy Management (RM). Skewed sensors do not have to be placed on orthogonal axes. The x, y, and z components of the sensed quantity can be determined using an appropriate coordinate transformation matrix. If one of the skewed sensors fails, the three orthogonal components can still be determined with another sensor and its transformation matrix.

A quad-redundant dual fail-operative system with orthogonal gyros in three axes requires twelve gyros. The same properly configured system with skewed gyros requires only six to maintain the same redundancy requirements. Skewing accelerometers can similarly reduce the number of sensors from twelve to six. Potential limitations are differences in scale and resolution requirements for each axis. For the skewed configuration, each gyro must have the same specifications. Depending upon the gyro chosen, either the signal quality may be limited or the instrumentation cost may be greater. Weinstein (1978) and Kaniuka, et al., 1982 show adequate performance for this technique.

Special sensors measure linear combinations of variables. The measurements are skewed in measurement space rather than geometrically, i.e., the sensor measures both acceleration and body rate. A conventional quad-redundant system could be replaced by five special sensors. These sensors are typically unique to the application and have a higher cost. A multipurpose air data sensor which measured pitot pressure, static pressure, angle of attack, and angle of sideslip was implemented in the system described by Weinstein (1978) and Kaniuka, et al., 1982.

Subsystem sensor integration can also be used to reduce the number of sensors. This technique uses data from subsystems which are not functionally related for monitoring and tie-breaking. An example is on the space shuttle where derived rates from the navigation system are used in the primary flight control system for voting.

Fault tolerant design can be achieved through in-line monitoring. The state-of-the-art for servos and computers is near 99 percent self-test confidence. In-line self-test feasibility for sensors is limited for several reasons. The sensor input is unknown except for special test signals. There is no way to test for sensor installation errors. Any sensor self-test adds considerable complexity which may be undesirable. Typically, a self-test can only detect very large faults, particularly in a dynamic environment.

Analytical Redundancy provides a means for substituting software algorithms for hardware sensors. Sensors are eliminated by analysis using known relationships between sensed values. Various simulation studies have shown the effectiveness of utilizing AR to increase system reliability and to reduce the amount of sensor hardware.

## 1.3. Scope

This document details the uses and limitations of analytical sensor redundancy. Section 2 gives an overview of AR. The physical relationships which can be utilized are written in equation form. The basic concept and building blocks are discussed. Section 3 describes various algorithms and design tools used to implement the filters used in AR processing. Its feasibility and performance are discussed in section 4. Algorithms and methods used for FD and isolation are detailed in section 5. Examples of the filters, RM, and sensor relationships for three cases where analytical sensor redundancy is easily implemented are given in section 6.

# 2. OVERVIEW

The basic idea of AR is to use known geometric and dynamic relationships between different sensors in order to detect and isolate sensor failures. These relationships can be defined in translational and rotational equations as shown in figures 2-1 and 2-2. Figure 2-2 also shows a diagram of the Euler angle relationships.

Cunningham and Hartmann (1977) describe the application of these mathematical relationships to eleven different measured quantities, normal acceleration, lateral acceleration, angle of attack, true airspeed, altitude, P, Q, R, Ø, $\theta$, and $\tau$.

Four categories of AR were utilized by Deckert, et al., 1978. Translational kinematics redundancy exists between the integrated accelerometer outputs, vertical and rate gyros, and the air data sensor outputs. Translational dynamics redundancy uses the aerodynamic forces on the aircraft measured by the accelerometers and stored coefficients to relate to aerodynamic forces calculated from air-data sensor data. Rotational kinematics redundancy relates the integrated outputs of the rate gyros and the vertical and directional gyro outputs. Altitude Kinematics (AK) redundancy is defined as the relationship between the altitude measured by the altimeter and the computed altitude from a double integration of the accelerometer and vertical gyro output data. These relationships are defined in the equations in figures 2-1 and 2-2. Examples of altitude and translational kinematics redundancy processing are given in sections 6.1 and 6.2.

## 2.1. Analytical Redundancy Building Blocks

Many specific approaches to AR have been developed, ranging from simple signal blenders to complex combinations of Kalman filters.

In general, AR is approached using one of two basic building blocks. A Diagnostic Filter (DF) is an algorithm which processes data from a family of N functionally related sensors in order to estimate signals and to assess the functioning of the sensors. It outputs signal estimates and an error flag which indicates that all sensors are functioning properly or that one of them has failed. A Super-Diagnostic Filter (SDF) performs the functions of a DF and can additionally isolate the specific faulted sensor. One can use assemblies of DFs to construct an SDF through truth table logic.

The concept of AR and associated FD are shown in figures 2.1-1 and 2.1-2.

Translational Equations

Inertial Velocity

$$\dot{X}_e = \cos\theta \cos\tau \; U + (\sin\emptyset \sin\theta \cos\tau - \cos\emptyset \sin\tau)V + (\cos\emptyset \sin\theta \cos\tau + \sin\emptyset \sin\tau)W$$

$$\dot{Y}_e = \cos\theta \sin\tau \; U + (\sin\emptyset \sin\theta \sin\tau + \cos\emptyset \cos\tau)V + (\cos\emptyset \sin\theta \cos\tau - \sin\emptyset \cos\tau)W$$

$$\dot{Z}_e = -\sin\theta \; U + \sin\emptyset \cos\theta \; V + \cos\emptyset \cos\theta \; W$$

Acceleration

$$\dot{U} = A_x - g \sin\theta - QW + RV$$

$$\dot{V} = A_y + g \cos\theta \sin\emptyset - RU + PW$$

$$\dot{W} = A_z + g \cos\theta \cos\emptyset - PV + QU$$

| | |
|---|---|
| where $X_e$, $Y_e$, $Z_e$ | = earth referenced forward, lateral, and vertical positions |
| U, V, W | = forward, lateral, and vertical body velocities, respectively |
| $A_x$, $A_y$, $A_z$ | = forward, lateral, and vertical body accelerations |
| g | = acceleration due to gravity |
| $\theta$, $\emptyset$, $\tau$ | = Euler pitch, roll, and yaw angles |
| P, Q, R | = body roll, pitch, and yaw rates |

FIGURE 2-1. TRANSLATIONAL RELATIONSHIPS USED IN ANALYTICAL REDUNDANCY

Rotational Equations

Euler Rates

$$\dot{\phi} = P + (Q \sin\phi + R \cos\phi) \tan\phi$$

$$\dot{\theta} = Q \cos\phi - R \sin\phi$$

$$\dot{\tau} = (Q \sin\phi + R \cos\phi) \sec\theta$$

Body Rates

$$P = \dot{\phi} - \dot{\tau} \sin\theta$$

$$Q = \dot{\theta} \cos\phi - \dot{\tau} \sin\phi \cos\theta$$

$$R = \dot{\tau} \cos\phi \cos\theta - \dot{\theta} \sin\phi$$

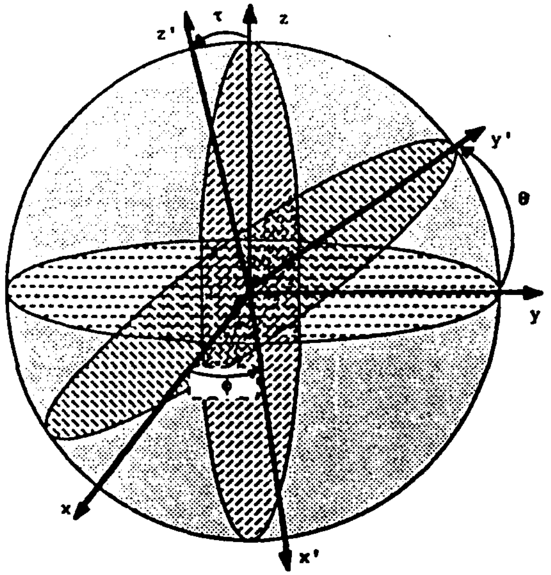
Moments

$$L = \dot{P}I_{xx} - \dot{R}I_{xz} + QR\,(I_{zz} - I_{yy}) - PQI_{xz}$$

$$M = \dot{Q}I_{yy} + PR\,(I_{xx} - I_{zz}) + (P^2 - R^2)\,I_{xz}$$

$$N = \dot{R}I_{zz} - \dot{P}I_{xz} + PQ\,(I_{yy} - I_{xx}) + QRI_{xz}$$

where $\theta$, $\phi$, $\tau$ = Euler pitch, roll, and yaw angles
$P$, $Q$, $R$ = body roll, pitch, and yaw rates
$L$, $M$, $N$ = moment about the body x, y, and z axes
$I_{xx}$, $I_{yy}$, $I_{zz}$ = moment of inertia about the x, y, and z axes
$I_{xz}$ = cross moment of inertia (xz axis)



EULER ANGLE DIAGRAM

FIGURE 2-2. ROTATIONAL RELATIONSHIPS USED FOR ANALYTICAL REDUNDANCY

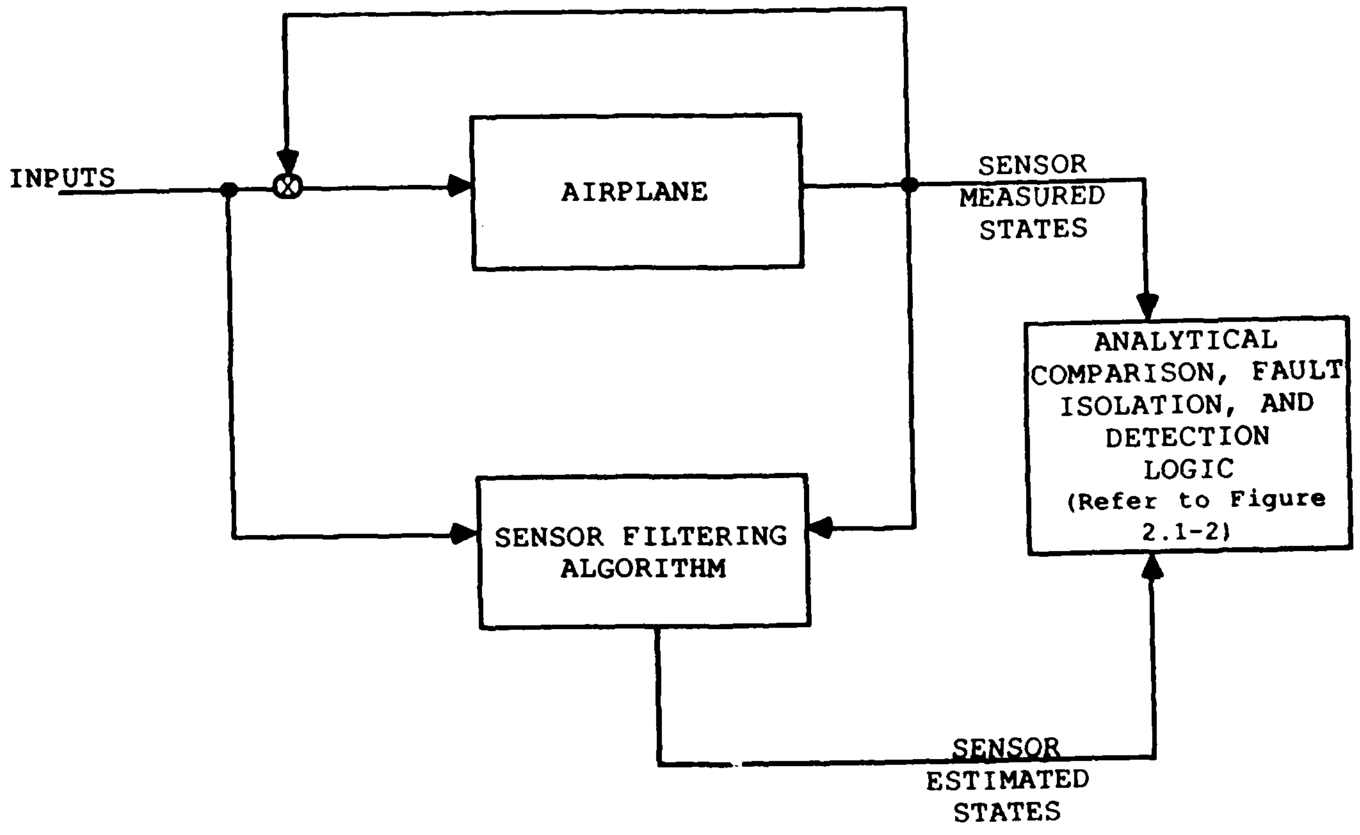
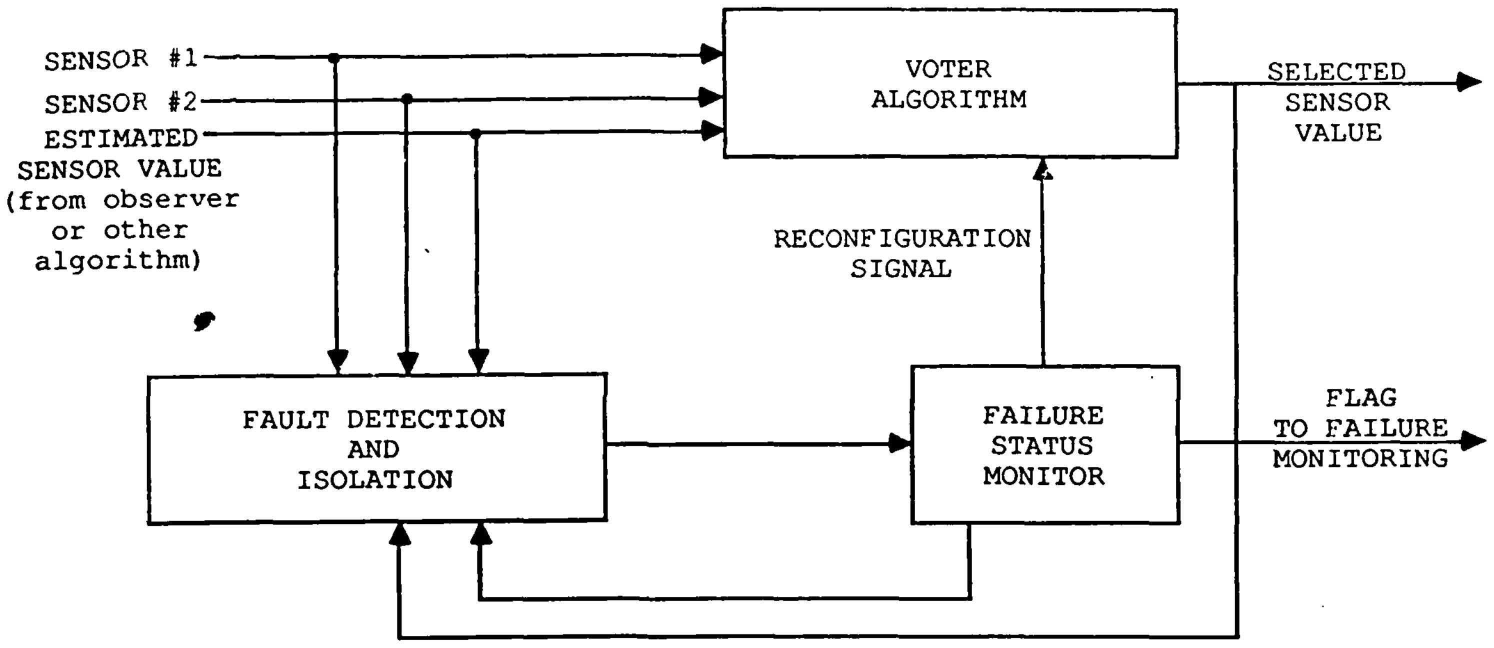

INPUTS
AIRPLANE
SENSOR FILTERING ALGORITHM
SENSOR MEASURED STATES
ANALYTICAL COMPARISON, FAULT ISOLATION, AND DETECTION LOGIC (Refer to Figure 2.1-2)
SENSOR ESTIMATED STATES

FIGURE 2.1-1. ANALYTICAL REDUNDANCY CONCEPT



SENSOR #1
SENSOR #2
ESTIMATED SENSOR VALUE (from observer or other algorithm)
VOTER ALGORITHM
SELECTED SENSOR VALUE
RECONFIGURATION SIGNAL
FAULT DETECTION AND ISOLATION
FAILURE STATUS MONITOR
FLAG TO FAILURE MONITORING

FIGURE 2.1-2. ANALYTICAL SENSOR REDUNDANCY FAULT DETECTION LOGIC

## 3. ANALYTICAL REDUNDANCY - DESIGN APPROACH

A literature survey was performed by Cunningham and Hartmann (1977) to examine currently available techniques that were able to detect and isolate faults in aircraft sensors and meet current onboard flight computer allocations. All such methods for failure detection were found to lie in three categories.

- Assemblies of DFs (see Meier, Ross, and Glaser, 1971; Maybeck, 1974; Hartmann, et al., 1975; and Clark, et al., 1975).

- Specific DF design techniques (see Kerr, 1974 and Mehra and Peschon, 1971).

- Explicit SDF design techniques.

The first two categories also include observer/blender techniques. Mulcare, Downing, and Smith (1987) and Deckert, et al., 1978 utilize these techniques.

The three filter types listed above can be combined in many ways to obtain useable AR results. The end product may vary considerably in accuracy and complexity. The structure of the filter depends on the overall RM approach, whether uniform redundancy or different levels of redundancy are required throughout the system.

Uniform redundancy schemes categorize sensors as interchangeable or noninterchangeable. Interchangeable sensors can substitute for each other when a failure occurs. Appropriate coordinate transformations must be accounted for, if necessary. If a noninterchangeable sensor fails, an identical one must replace it in order to maintain performance.

If N fully operational sensors are required to maintain aircraft operations, then a minimum of N+2 interchangeable sensors and 3N noninterchangeable sensors are required for dual fail-operational performance when using AR. In order to resolve conflicts using traditional voting techniques, N+3 and 4N sensors are needed to maintain the same performance.

Fault Detection using DFs with interchangeable sensors is illustrated in figure 3-1. The figure shows FD for N, the number of sensors required for safe flight, equal to 2 for fail-operational performance. The truth table shows that each column of the error flags is a unique binary word and that the sensor inputs to each filter are uniquely determined by each row of the table. The generalized way to assemble DFs for interchangeable sensors is given below.

- Determine the number of sensors required to maintain safe flight and meet operational requirements (N is the number of sensors necessary for safe flight).

N + 1 for fail-operational performance
N + 2 for dual fail-operational performance

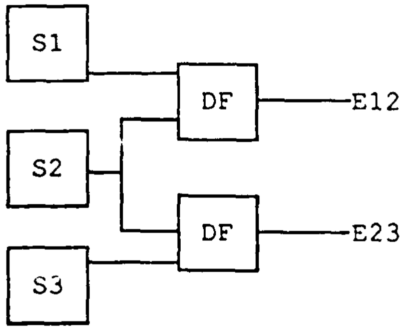
- Determine the number of DFs (the brackets indicate to use the next largest integer of the enclosed expression).

$[\log_2 (N + 2)]$ for fail-operational performance
$[\log_2 (N + 3)]$ for dual fail-operational performance

- Determine sensor inputs to each filter from the truth table.

The FD capability of a DF combined with comparators for noninterchangeable sensors can also be verified with a truth table. See figure 3-2 for an illustration of fail-operational performance with N, the number of sensors necessary to maintain safe flight, equal to 2. The generalized arrangement uses one filter and N comparators for fail-operational and one filter and 2N comparators for dual fail-operational. The truth table here contains FD for single sensor failures only. It is generally assumed that failures occur singly when designing FD algorithms. A single SDF is all that is needed in all cases to provide FD and isolation. This type of filter may be quite complex in order to achieve the same results as DFs.

INTERCHANGEABLE SENSORS
for N=2 and fail-operational performance



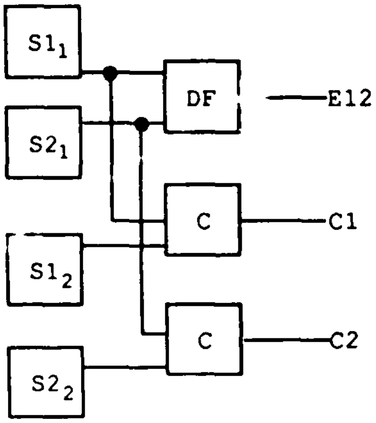
TRUTH TABLE

| | SINGLE SENSOR FAILURE | | | |
|---|---|---|---|---|
| ERROR FLAGS | NONE | S1 | S2 | S3 |
| E12 | 0 | 1 | 1 | 0 |
| E23 | 0 | 0 | 1 | 1 |

FIGURE 3-1. EXAMPLES OF FAULT DETECTION USING DIAGNOSTIC FILTERS AND INTERCHANGEABLE SENSORS

NONINTERCHANGEABLE SENSORS

for N=2 and fail-operational performance



TRUTH TABLE

| | SINGLE SENSOR FAILURE | | | | |
|---|---|---|---|---|---|
| ERROR FLAGS | NONE | $S1_1$ | $S2_1$ | $S1_2$ | $S2_2$ |
| E12 | 0 | 1 | 1 | 0 | 0 |
| C1 | 0 | 1 | 0 | 1 | 0 |
| C2 | 0 | 0 | 1 | 0 | 1 |

C = Comparator
DF = Diagnostic Filter
N = # of sensors needed to maintain safe flight

FIGURE 3-2. EXAMPLES OF FAULT DETECTION USING DIAGNOSTIC FILTERS AND NONINTERCHANGEABLE SENSORS

The largest amount of sensor reduction is achieved for noninterchangeable sensors when using AR. In this case, AR implemented with one DF in combination with 2N comparators has the same benefit as one SDF. An SDF which is more complex will not be feasible. A comparison of the sensor reductions possible with these analytical techniques and traditional voting is given in table 3-1. The number of comparators and DFs needed for AR are also given. N is defined as the minimum number of sensors required to maintain safe flight.

There is a sensor reduction benefit for interchangeable sensors; however, it is a small one. AR provides little or no benefit to save one sensor. More DFs are needed to match the capabilities of a single SDF than for noninterchangeable sensors.

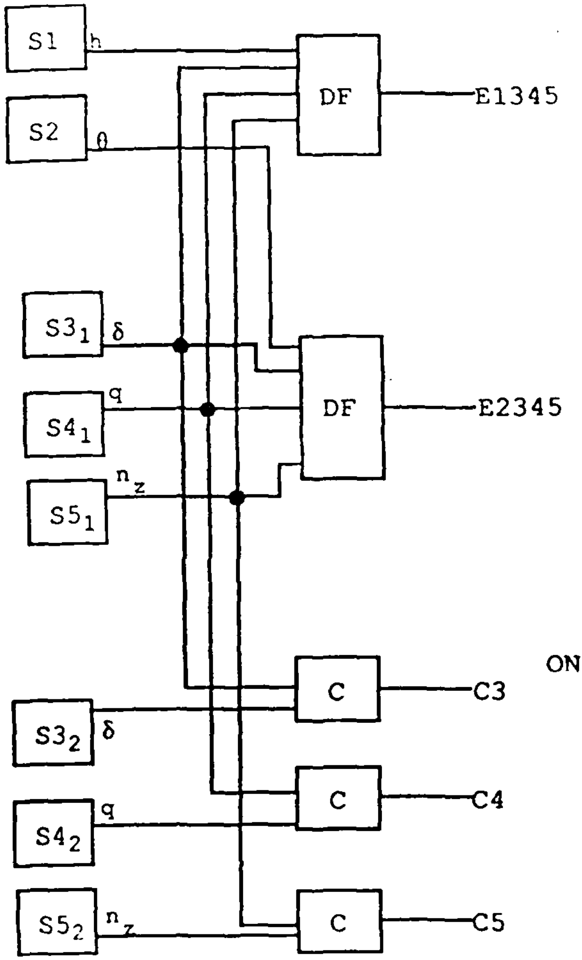
Current flight control systems normally do not have the same redundancy requirements for all sensors. A more realistic setup may have high levels of redundancy for some critical sensors and lower levels for others. The high levels of redundancy are known as reversion modes. While this may be application dependent, the basic principles can be used to obtain a failure detection scheme as shown in figure 3-3. In order to implement the reversion modes, sufficient filters are required to distinguish between four outer loop logic conditions: no failure; S1 failed; S2 failed; and $S3_1$, $S4_1$, or $S5_1$ failed. The error flags, E1345 and E2345, are used to obtain this information. The error flags, C3, C4, and C5, must be used to determine which of the inner loop sensors have failed.

TABLE 3-1. SENSOR REDUCTION COMPARISONS FOR ANALYTICAL REDUNDANCY BUILDING BLOCKS

| **FAIL-OPERATIONAL** | NUMBER OF SDF'S | NUMBER OF DIAGNOSTIC FILTERS | NUMBER OF COMPARATORS | NUMBER OF SENSORS |
|---|---|---|---|---|
| **INTERCHANGEABLE SENSORS** | | | | |
| DETECTION WITH SDF'S | 1 | 0 | 0 | N+1 |
| WITH DF'S | 0 | $[\mathrm{LOG}_2(N+2)]$ | 0 | N+1 |
| WITH VOTING | 0 | 0 | N+3 | N+2 |
| **NONINTERCHANGEABLE SENSORS** | | | | |
| DETECTION WITH SDF'S | 1 | 0 | 0 | 2N |
| WITH DF'S | 0 | 1 | N | 2N |
| WITH VOTING | 0 | 0 | 2N | 3N |
| **DUAL FAIL-OPERATIONAL** | NUMBER OF SDF'S | NUMBER OF DIAGNOSTIC FILTERS | NUMBER OF COMPARATORS | NUMBER OF SENSORS |
| **INTERCHANGEABLE SENSORS** | | | | |
| DETECTION WITH SDF'S | 1 | 0 | 0 | N+2 |
| WITH DF'S | 0 | $[\mathrm{LOG}_2(N+3)]$ | 0 | N+2 |
| WITH VOTING | 0 | 0 | N+4 | N+3 |
| **NONINTERCHANGEABLE SENSORS** | | | | |
| DETECTION WITH SDF'S | 1 | 0 | 0 | 3N |
| WITH DF'S | 0 | 1 | 2N | 3N |
| WITH VOTING | 0 | 0 | 3N | 4N |

N = MINIMUM NUMBER OF SENSORS REQUIRED FOR SAFE FLIGHT

[ ] IMPLIES USE THE NEXT LARGEST INTEGER OF THE EXPRESSION WITHIN THE BRACKETS



TRUTH TABLE

| ERROR FLAGS | SENSORS FAILED<br>NONE | S1 | S2 | $S3_1$ | $S4_1$ | $S5_1$ | $S3_2$ | $S4_2$ | $S5_2$ |
|---|---|---|---|---|---|---|---|---|---|
| E1345 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| E2345 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| C3 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| C4 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| C5 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

TWO FAIL-SAFE OUTER LOOPS (h), (θ)

ONE FAIL-OPERATIONAL INNER LOOP ($\delta, q, n_z$)
(NON-INTERCHANGEABLE SENSORS)

h - altitude
θ - Euler pitch angle
δ - control surface deflection
q - body pitch rate
$n_z$ - normal acceleration
C - Comparator
DF - Diagnostic Filter

FIGURE 3-3. EXAMPLE OF FAULT DETECTION WITH REVERSION MODES

Three concepts encompass the categories of failure detection methods. These are examined as a result of various combinations of DFs. These concepts in order of increasing complexity are:

- Observer/signal blender filter.
- Diagnostic Kalman filters.
- Super-diagnostic Kalman filter design.

### 3.1. Observer/Signal Blender Filter

An observer/blender will model physical relationships using sensor outputs to provide FD for several sensors. It uses a specific DF design and has the least amount of complexity and computer requirements. Monitors may use a three trip level exceedance criterion to detect failures. Trip thresholds can be set to account for unmodeled dynamics and sensor anomalies.

The basic operation of the observer/blender is to define a consistent error function between a measured parameter and its derivative. Both values are measured for all but a few parameters, e.g., lateral acceleration. A relationship such as,

$$V_x = \dot{X}$$

is exact. For perfect measurements, there is no error. Realistically, the measured values of $V_x$ and X are not true representations of $V_x$ and X. There is an error associated with digital integration and sampling. Either $V_x$ or X may contain faults. This implementation of AR must distinguish between the errors associated with measurements and digital sampling and errors associated with the sensors.

### 3.2. Diagnostic Kalman Filters

Diagnostic Kalman filters incorporate modeling of sensor anomalies (such as, bias, scale factors, and wind gust estimation) in the filter. FD is provided for more sensors than available with the observer/blender. This is achieved by using an assembly of DFs. This concept places moderate requirements on a computer.

### 3.3. Super-Diagnostic Kalman Filter Design

The super-diagnostic design utilizes Kalman filters as well as linear equations for pitch and lateral directional dynamic equations of motion. Both detection and isolation can be determined. An error signal is created for each sensor involved. The concept is built with an assembly of DFs. Some applications may be very complex.

The largest number of surveyed references are devoted to this topic. These filters are the most difficult to construct. They are constrained more than other techniques due to the amount of complexity which is feasible. Five methods have been examined for SDFs.

- Multiple hypothesis test.
- Parameter identification.
- Generalized likelihood ratio methods.
- Modified filter designs.
- Jump process estimation.

### 3.3.1. Multiple Hypothesis Tests

Each failure condition of a particular sensor is used to define a hypothesis. The entire range of failure conditions forms a set of hypotheses which are tested against observed data. One Kalman filter is required to test each hypothesis. The filter generates residuals, assuming that the hypothesis is true, which are summed into likelihood functions. The maximum likelihood then identifies the current valid hypothesis. This results in a large number of filters for even a few sensors and at present is too complex for advanced flight computers to utilize. Montgomery and Caglayan (1974), Montgomery and Price (1974), Athans and Willner (1973), Lainiotis (1971), and Buxbaum and Haddad (1969) contain more information.

### 3.3.2. Parameter Identification

Parameters of each sensor, such as, gain and bias, are defined as unknowns and estimated from sensor data. If the estimates deviate a great deal from nominal values, then a failure is declared. For any procedure used, a separate calculation similar to a Kalman filter is required to compare the nominal values with the estimated sensor parameters. This becomes as complex and inefficient as the previous technique. Mehra and Peschon (1971) and Stein and Hartmann (1976) have investigated this technique.

### 3.3.3. Generalized Likelihood Ratio Methods

In an attempt to reduce the complexity of this type of failure detection method, initial constraints were placed on the design of an algorithm. These constraints are that only one Kalman filter is available and that sensor failure detection must be decided through the monitoring of residuals from the single filter. This can be done for those failures which have recognizable signatures for correlation processing. The residuals are correlated with known signals, normalized by their expected no-failure value, and compared to predetermined threshold levels. The number of filters has been greatly reduced, however, the correlation functions can be fairly complex. See Willsky, Deyst, and Crawford (1974); Willsky and Jones (1974), Deyst and Deckert (1975), McAulay and Denlinger (1973), and Sanyal and Shen (1974).

### 3.3.4. Modified Filter Design

This method starts with a constraint of one Kalman filter. It does not allow the filter to remain a fixed element. An attempt is made to alter the filter gains to produce strong and easily recognized failure signatures. This concept is largely theoretical at this time. Details are given in Jones (1973) and Beard (1973).

### 3.3.5. Jump Process Estimation

This procedure is also theoretical. The basic idea is to represent failures as random jump processes in an otherwise known stochastic system. The time of occurrence and magnitude of the jumps are then estimated using optimal stochastic filtering theory. (See Sworder, 1972; Sworder and Robinson, 1973; Ratner and Luenberger, 1969; Pierce and Sworder, 1971; Davis, 1975; McGarty, 1974; and Chien, 1972.)

## 3.4. Redundancy Management

Redundancy Management will be optimized when included in a system design, but it can be incorporated into an existing system. Mulcare, Downing, and Smith (1987) modified an existing quadruplex DFCS to incorporate AR. Section 6.3 contains example filters which could be used to add AR to one of the functions, a Stability Augmentation System (SAS), implemented in this modification.

Issues concerned when designing and structuring the RM are:

- The number of success paths.
- The amount of dependency placed on monitoring quality.
- The tradeoff between fail safety and reliability.
- The cost effectiveness for increased reliability with added FD and isolation.
- The throughput constraints imposed by the flight computer. RM can be 60 to 80 percent of the required processing.

Performance qualities may vary for different RM structuring.

In order to maintain fail-safe sensor operations, the following three types of logic are needed.

- Comparison monitoring of dual like signals without an associated DF. Examples where this may be implemented are after a computer failure or a failure of an input to a DF.
- Monitoring the diagnostic error function after failure of one-out-of-two sensors in a dual set. If a pitch rate gyro fails, the relevant DF then monitors the remaining pitch rate gyro.

- Monitoring of a single sensor by its associated DF. This logic requires a failure declaration from both computers to avoid fault indication due to a dual sensor failure.

## 4. ANALYTICAL REDUNDANCY - RELIABILITY

The concept of AR, in order to be implemented in practice, must satisfy performance and reliability requirements of typical flights and must not overload the flight computer.

The traditional RM for a quadruplex set of sensors would isolate the first and second failed sensors by a majority vote. On the failure of the third sensor the set would be shut down. For a perfect monitoring process, the probability of total failure of the set is $4Q_s^3$, where $Q_s$ is the probability of failure of one of the sensors within a certain time. The probability of any two sensors failing is $6Q_s^2$.

A rate gyro has a failure rate of about $10^{-4}$ per hour. This is one of the worst sensor failure rates. The probability of a quadruplex set of gyros failing would be $4 \times 10^{-12}$. This exceeds the typical flight control system requirements per sensor set of $10^{-9}$ by more than two orders of magnitude. For a triplex set of gyros, failure is defined as $3Q_s^2$ with a value of $3 \times 10^{-8}$ which is less than the requirements by a factor of thirty.

The assumption of perfect monitoring is not valid. An additional factor, $Q_m$, should be included in the failure rate. $Q_m$ defines the probability that the first failure is not detected and that both failures are alike. This issue of imperfect monitoring or coverage may cause failure of a quadruplex sensor set after only two failures, if it cannot distinguish between the two good and two failed sensors. The probability of failure here is $6Q_s^2\ Q_m$. No data exists for the term $Q_m$, but numbers on the order of $10^{-2}$ have been suggested. With imperfect monitoring, the probability of failure for a quadruplex set of rate gyros is $6 \times 10^{-10}$ in one hour which is just within the requirements.

The diagnostics provided in an AR system must provide similar quality in monitoring. For triplex sensors configured for dual-fail-operational systems, the total failure rate is given in the following equation.

$$Q_s^3 + 3Q_s^2\ Q_d$$

The first term represents the probability for all three sensors failing. The second term is the combination of the probabilities of a dual sensor failure and the diagnostics failing to recognize the fault, $Q_d$. This is the dominant term. If it is set equal to the reliability requirement,

$$3Q_s^2\ Q_d - 10^{-9}$$

$$Q_d - 3.3 \times 10^{-2}$$

The value of $Q_d$ indicates that the diagnostics must be 97 percent reliable. If this performance is feasible, then AR techniques are at least equal to those of quadruplex channel voting.

This example was devoted to just one set of sensors. Total system reliability includes all hardware: computers, servos, and sensors. A computer code, Computer Aided Redundant System Reliability Analysis (CARSRA), computes system reliabilities based on a specific configuration and sensor failure rates. Mulcare, Downing, and Smith (1987) used a revised version of this code to perform a system reliability assessment.

Table 4-1, utilizing parameters of an existing system (Cunningham and Hartmann, 1977), shows that servos, not sensors, tend to dominate reliability. By adding sensor redundancy, only a factor of two less than baseline system failure rate is obtained. With both sensor and servo redundancy, system failure rate decreased by more than an order of magnitude. Failure rates are dependent on system architecture. A system should be designed to have matched reliability.

TABLE 4-1. SYSTEM RELIABILITY

| Probability (failures per flight hour) | | |
|---|---|---|
| Failure Type | 95% Sensor Redundancy | 95% Sensor/Servo Redundancy |
| Either computer fails (95% effective self-test) | $0.2 \times 10^{-4}$ | $0.2 \times 10^{-4}$ |
| Servo failure in any axis | $6.0 \times 10^{-4}$ | $0.3 \times 10^{-4}$ |
| Gyro failure in any axis | $0.3 \times 10^{-4}$ | $0.3 \times 10^{-4}$ |
| Normal accelerometer failure | $0.02 \times 10^{-4}$ | $0.02 \times 10^{-4}$ |
| Total | $6.52 \times 10^{-4}$ | $0.82 \times 10^{-4}$ |

## 5. ANALYTICAL REDUNDANCY - FAULT DETECTION AND ISOLATION

The type of FD monitor used to test various error signals is critical for performance. Important parameters are speed of response and an acceptable false alarm rate, one per 1000 hours of flight. Observers or DFs can operate with comparison monitors of dual sensors to isolate faults for a fail-operational capability. A fail-safe capability exists for all single sensors and for dual sensors after one failure.

Fault Detection monitors can be multiple trip monitors or a Sequential Likelihood Ratio Test (SLRT) of a defined parameter, error signals, or likelihood functions. The design goal of an FD monitor is FD within a minimum time after the occurrence of the fault while maintaining an acceptable false alarm rate. Another important goal is the number of missed alarms. This is addressed in the literature (Cunningham and Hartmann, 1977 and Deckert, et al., 1978) where data exists from flight simulation tests.

### 5.1. Multiple Trip Monitor

The FD logic in a multiple trip monitor typically requires three consecutive trips for a fault to be declared. The trip thresholds must be based on the performance of each sensor and known sensor and modeling inaccuracies.

The simplest test to check for an error signal is to compare its magnitude with predefined limits. This is illustrated in figure 5.1-1. The trip magnitude is typically placed at some multiple, m, of $\sigma$, the standard deviation of the error signal of an unfailed sensor. The mean of this error signal is zero. The value of m is chosen to yield an acceptable false alarm rate. This is shown in the following sequence of equations. The probability that there will be no false alarms during one hour of flight is given by a Poisson distribution. See Ross (1972) for more information on probability density functions, likelihood functions, and reliability.

$$P(\text{no false alarms}) = e^{-\delta t}$$

where $\delta$ = the false alarm rate (1 per 1000 flight hours)
t = the flight time (1 hour)

so that P(no false alarms) = 0.999. This is also equal to the probability that a sequence of random variables, the sampled error signals, will remain within the trip boundary of $m\sigma$.

$$P\left(\bigcap_{i=1}^{n} X_i\right) = e^{-\delta t}$$

For a one hour flight, sampling at 16 Hz, n will equal 57,600.

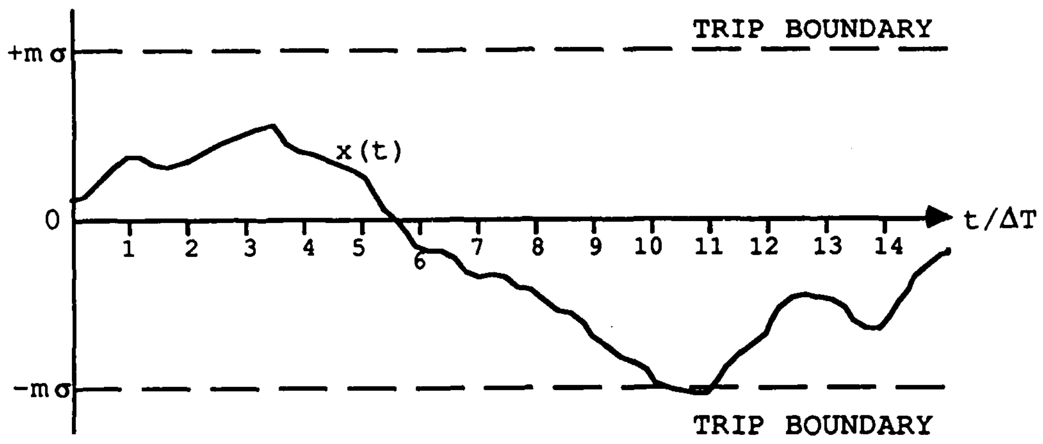


FIGURE 5.1-1. MULTIPLE TRIP FAULT DETECTION MONITOR

If the sequence of random numbers is independent, then

$$P(\bigcap_{i=1}^{n} X_i) = \mathop{\pi}_{i=1}^{n} P(X_i\ ) = nP(X_i)$$

$$P(|X_i| > m\sigma) = (1 - e^{-\delta t}) / n$$

$$= 1.74 \times 10^{-8}$$

This would require m to be much larger than 4. Multiples of $\sigma$ are not given in normal probability tables for numbers in this range. For three consecutive trips,

$$P(|X_i| > m\sigma;\ \text{for three consecutive times}) = (1.74 \times 10^{-8})^{1/3}$$

$$= 2.6 \times 10^{-3}$$

This corresponds to $m \approx 3.2$. This multiple of $\sigma$ was determined using a table containing probability values for a standard normal distribution.

For a completely dependent sequence,

$$P(|X_i| > m\sigma;\ \text{for three consecutive times}) \approx P(|X_i| > m\sigma;\ \text{one time})$$

$$\approx 1 - e^{-\delta t}$$

$$= 1.0 \times 10^{-3}$$

This corresponds to $m \approx 3.4$. This value was obtained from the same table used above.

The results of this analysis imply that the triple trip boundary needs to be set at $3.4\sigma$ to meet the false alarm rate for a given error signal.

The trip threshold can remain constant, adjusted based on the output of the sensor, or adjusted based on inputs from the pilot. An adjustable threshold can increase sensitivity to environmental disturbances, such as turbulence, and to aircraft in-flight maneuvering.

A multiple trip criterion (i.e., a fault is declared when a limit is exceeded n consecutive times) gives a much lower false alarm rate than a first trip monitor. The number of consecutive trips chosen for a monitor is a tradeoff between error insensitivity and the speed of FD. Choosing a multiple number of trips applies a built-in delay to FD.

## 5.2. Sequential Likelihood Ratio Tests

Likelihood ratio tests have been demonstrated to be a better FD scheme than the multiple trip monitor in Cunningham and Hartmann (1977). This algorithm provides quicker response to faults such as hardover, and more sensitivity to other smaller faults (bias and scale factor changes). However, there is more complexity to this monitoring scheme.

These tests are based on two hypothesized density functions of a random variable, $f_0(x)$ and $f_1(x)$. The likelihood ratio is expressed as a function, $\Gamma_n$, of error signal observations of that random variable.

$$\Gamma_n = \frac{f_0(e_1, e_2, \ldots, e_n)}{f_1(e_1, e_2, \ldots, e_n)}$$

The two hypothesized outcomes, $H_0$ and $H_1$, are no failure or sensor failure. These outcomes are accepted based on the following rules.

- Accept $H_0$ if $\Gamma_n \leq A$.

- Accept $H_1$ if $\Gamma_n \geq B$.

- No decision if $A < \Gamma_n < B$.

where A = 1/B. A typical value for B is 20,000.

$H_0$ implies that the expected value of a given error signal is 0 and there is no fault. $H_1$ implies the mean of the error signal has shifted unacceptably to $\mu_1$ and a sensor fault should be declared. For actual monitoring, a combined test is used where $\mu_1$ may equal $\pm m\sigma$. Figure 5.2-1 illustrates the bounds for $H_0$ and $H_1$.

This can be defined mathematically using the following equations. The functions, $f_0$ and $f_1$, are assumed to have a normal distribution with a standard deviation of $\sigma$.

$$f_0(e_i) = c \exp[-\sum_{i=1}^{n} (e_i - \mu_0)^2 / 2\sigma^2 ]$$

$$f_1(e_i) = c \exp[-\sum_{i=1}^{n} (e_i - \mu_1)^2 / 2\sigma^2 ]$$

Using the no decision criteria, taking natural logarithms, and substituting 0 for $\mu_0$ and $\pm m\sigma$ for $\mu_1$,

$$\ln A < \sum_{i=1}^{n} [(e_i \mp m\sigma)^2 - (e_i)^2 ] / 2\sigma^2 < \ln B$$

which is equivalent to

$$nm\sigma/2 - \sigma \ln B/m < \sum_{i=1}^{n} e_i < nm\sigma/2 + \sigma \ln B/m, \text{ for } \mu_1 = +m\sigma$$

and

$$-nm\sigma/2 - \sigma \ln B/m < \sum_{i=1}^{n} e_i < \sigma \ln B/m - nm\sigma/2, \text{ for } \mu_1 = -m\sigma$$

A fault is determined when $\left|\sum_{i=1}^{n} e_i\right| \leq \sigma \ln B/m + nm\sigma/2$.

No fault is determined when $\left|\sum_{i=1}^{n} e_i\right| \geq nm\sigma/2 - \sigma \ln B/m$.

Otherwise, no decision is made.

The test sequence begins by initializing n to 1 and updates the summation each cycle. The sequence restarts when $H_0$ is accepted or there is no decision for a fixed period of time. Frequent restarts are desirable because summations over long intervals have less sensitivity to new data.

Likelihood functions of like sensors, i.e., with identical statistical error characteristics, can be compared and used to isolate the faulted sensor. The likelihood functions are $L_{n1}$ and $L_{n2}$ for sensors 1 and 2, respectively. The hypotheses here are that $H_0$ implies that sensor 1 has failed, and $H_1$ implies that sensor 2 has failed. The mean of $H_0$ is $\mu_0$ which is equal to $+m\sigma$, and the mean of $H_1$ is $\mu_1$ which is equal to $-m\sigma$.

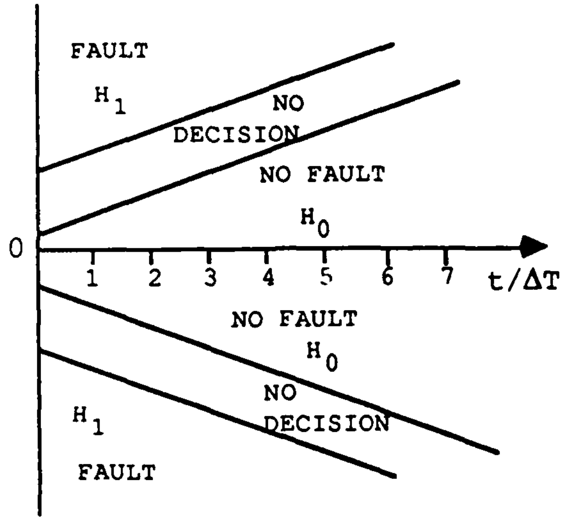


FIGURE 5.2-1. SEQUENTIAL LIKELIHOOD FAULT DETECTION MONITOR

Decisions are made using the difference of the likelihood functions based on the following rules.

$\Delta L_n = L_{n1} - L_{n2}$

- Accept $H_0$ if $\Delta L_n \geq \sigma \ln B/2m$.
- Accept $H_1$ if $\Delta L_n \geq \sigma \ln A/2m$.
- No decision if $\sigma \ln A/2m < \Delta L_n < \sigma \ln B/2m$.

Because the no fail hypothesis is not included here, this particular test can proceed only when a fault has already been declared. This test can be initiated after one trip using comparison monitoring. If a fault is declared (three consecutive trips), then the likelihood comparison test is used to determine which sensor is faulted. Because the likelihood functions can only increase in a fault situation, the plus or minus direction of the delta likelihood function provides the information necessary to determine which sensor has failed.

## 5.3. Fault Modeling

Sensor error and fault modeling require careful treatment for FD because typical sensor models are not sufficient and fault characteristics may not be well-defined. A key issue is modeling sensor characteristics, including noise in an operational environment. Possible errors superimposed on the sensor output include bias, resolution, scale factor, null output, alignment error, hysteresis, environmental effects, response dynamics, and unmodeled sensor inputs. Errors may occur if the model does not include pilot inputs. Mode specific error signals may occur for selected modes, e.g., altitude or heading hold. A determination of the importance of each type of error is dependent on the type and percentage of occurrence of failure modes for each sensor. Modeling these errors may be a difficult task, because data is not easily obtained or does not exist on some of these parameters.

Faults can be classed as open-loop or closed-loop faults. An open-loop fault is one in which the sensor output is completely independent of its input. Examples of this category are hardover (at maximum output), zero output, output stuck at an intermediate value, and a randomly varying output. Closed-loop faults consist of the correct sensor output with errors superimposed. These faults are misalignment, scale factor changes, noise, or others listed in the previous paragraph.

Simulations should subject the FD algorithms to the highest probability faults. Sensor hardover, dead sensor, dynamic response reduction, scale factor changes, and bias shifts represent 90 to 95 percent of expected failures in typical rate gyros and accelerometers. These two sensor types have the highest failure rates compared to other sensors. Other faults should be defined dependent on the sensor.

Some techniques are limited in the type of failures they look for. Deckert, et al., 1978 limited their technique to looking for bias failures. They felt that most other failures could be found with the same technique. As yet, no one has addressed oscillatory faults which may or may not be important.

As defined by Cunningham and Hartmann (1977), the observer/blender and diagnostic Kalman filter worked well for FD for most sensors included in the study. Super-diagnostic techniques were found to have performance concerns and developmental needs. Problems arose in detection of accelerometer soft failure, dynamic response faults, and FI based on more than one filter detecting a given fault. (The difficulty arose when both filters did not detect the failure at the same time.)

A comparison of monitors shows that the SLRT of residual mean values performed well relative to the multiple trip monitor. SLRT caught hardover failures sooner. Frequently scale factor changes would escape the multiple trip monitor, but not the SLRT.

One way to enhance a particular FD algorithm is to utilize the fact that there are physical limitations as to how much the aircraft state can change from one sample to the next. This can minimize the effects of extremely large sensor failures. Desai, Deckert, and Deyst (1979) added a self-test in conjunction with an FD algorithm which provisionally failed a sensor when an abrupt change in output was maintained for three sample intervals.

# 6. SUPPLEMENTAL WORKED EXAMPLES

## 6.1. Altitude Kinematics

Altitude Kinematics refers to the redundancy between changes in altitude measured by the barostatic pressure sensors and changes in altitude computed from the vertical acceleration measured by the accelerometers. The vertical direction is determined via Euler attitude angles: roll ($\emptyset$) and pitch ($\theta$). Since the accelerometers sense gravity, the gravitational component must be subtracted in computing vertical acceleration. Vertical acceleration is computed as:

$$A_v = A_x \sin\theta - (A_y \sin\emptyset + A_z \cos\emptyset) \cos\theta - g$$

where $A_x$, $A_y$, $A_z$ are measured accelerations compensated to the center of mass.

A third order complementary filter (illustrated in figure 6.1-1) is used to store $\dot{h}$ (vertical velocity) prior to a failure detection and possible corruption. The value of $\dot{h}$ can then be used to compare altitude deviation from slightly prior to the failure detection by keeping a moving window of data.

The altitude residues for both sensors would be:

$$\text{Residue \#1} = \Sigma(\text{current } h_1 - \text{previous } h_1 - \dot{h}\, dt)$$

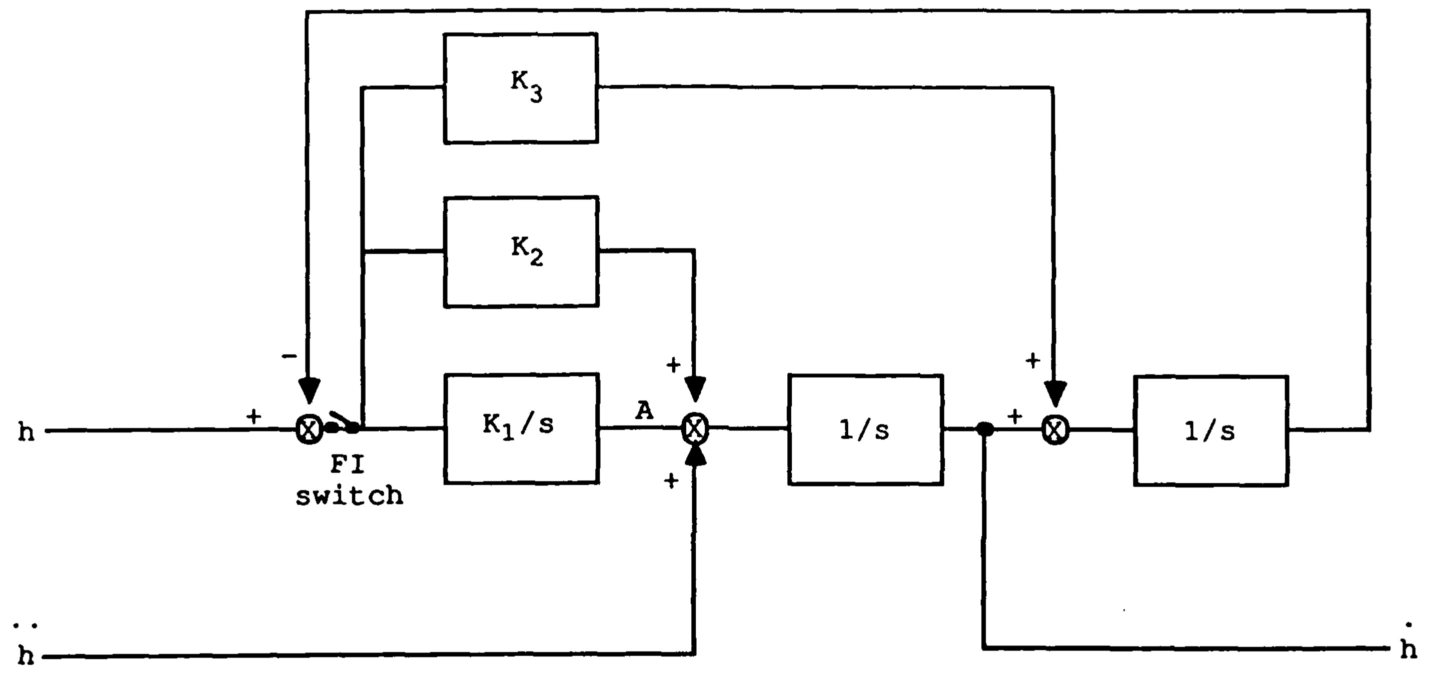
$$\text{Residue \#2} = \Sigma(\text{current } h_2 - \text{previous } h_2 - \dot{h}\, dt)$$

using h measurements from sensors 1 and 2, respectively, where dt is the integration interval.

Both residues are then evaluated by an FI algorithm. The algorithm may be a multiple trip threshold exceedance or a statistical hypothesis algorithm (e.g., SLRT).

During the FI period, the $\dot{h}$ used is only inertially updated via the switch shown in figure 6.1-1, i.e., $\dot{h} = \int \ddot{h}$. The switch opens (FI begins) when the absolute magnitude of $(h_1 - h_2)$ exceeds a threshold N times. The filter is not updated if any sample exceeds the threshold to avoid $\dot{h}$ corruption. Figure 6.1-2 demonstrates the RM processing.

Error sources must be evaluated to avoid a false FI decision. The third order filter has a state to estimate steady-state errors on $\ddot{h}$ to avoid a parabolic error growth when calculating both residues. An error analysis must be made to determine the maximum time that can be allowed for FI.



h is the average of
two baro-static
pressure altitudes

A is an estimate of error of $\ddot{h}$,
subsequently added to each $\ddot{h}$ calculation
in the fault isolation residue equations
to effectively cancel the error.

FIGURE 6.1-1 THIRD ORDER VERTICAL COMPLEMENTARY FILTER FOR ALTITUDE KINEMATICS

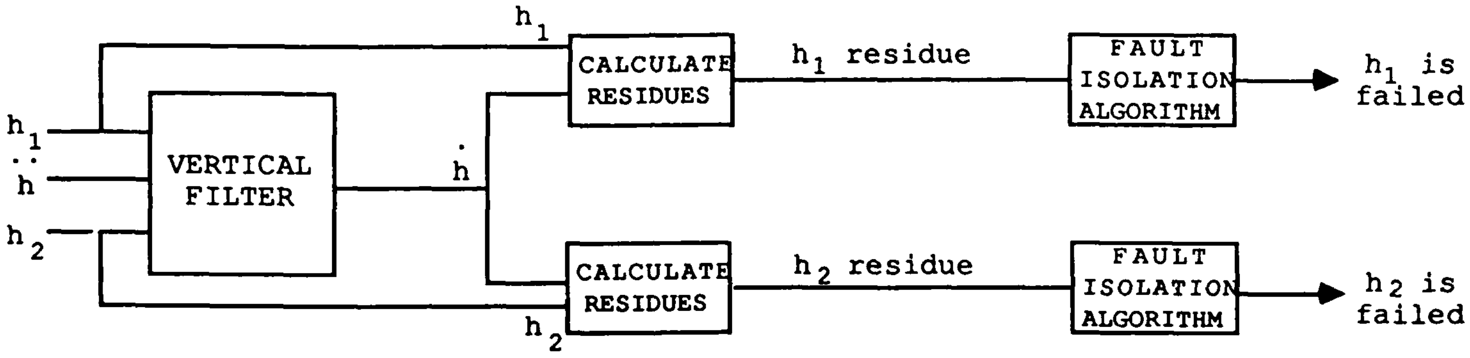


FIGURE 6.1-2. POSSIBLE REDUNDANCY MANAGEMENT FOR ALTITUDE KINEMATICS FAULT ISOLATION

If the time expires without an FI decision, then the following logic can be used:

Is there still a fault?

The answer is yes, if the absolute magnitude of $(h_1 - h_2)$ is greater than the threshold. Then isolate the sensor with the worst error history, i.e., the largest residue magnitude.

Otherwise, the answer is no. Reset the RM logic and restart the vertical filter, closing the FI switch and clearing the FD flag, if one is present.

6.2. Translational Kinematics

A translational kinematic relationship can be used to determine an airspeed sensor fault by means of the related inertial acceleration along the x-axis, such that

$$V_x = \int \dot{U}\,dt \qquad \text{or} \qquad \Delta V_x = \dot{U}\,dt$$

$$V_x = V_t \cos\beta \cos\alpha \approx V_t \qquad \text{for small angles of } \alpha \text{ and } \beta$$

where $V_x$ = x-axis airspeed velocity

$V_t$ = true airspeed

$\alpha$ = angle of attack

$\beta$ = angle of sideslip

$U$ = inertial velocity along the x-axis

An estimate of $\dot{V}_x$ can be obtained using the following equation.

$$\dot{V}_x = A_x - g \sin\theta - QW + RV + \delta_x$$

where $Q$ = pitch rate

$W$ = z-axis velocity

$R$ = yaw rate

$V$ = y-axis velocity

$\delta_x$ = wind acceleration along the x-axis

$A_x$ = acceleration measured by axial accelerometer

Q and R are measured gyro values. V and W can be calculated as follows.

$V = V_t \sin\beta \quad = \text{y-axis velocity}$

$W = V_t \cos\beta \sin\alpha \quad = \text{z-axis velocity}$

The only term unaccounted for is $\delta_x$, wind acceleration. It must be carefully analyzed as an error source in the FI decision. As long as the FI period is not too long relative to this error source, the decision should not be wrong.

Another way to alleviate this error source is to use a moving window to calculate the standard deviation of the airspeed residues (prior to FD) to determine the threshold size for FI. Wind turbulence associated with wind acceleration increases the threshold, thereby protecting from a false FI.

A filter is used to get a good estimate of any steady-state error on $\dot{V}_x$ as shown in figure 6.2-1. The term a is an estimate of error on $V_x$, subsequently added to each $V_x$ calculation in the FI residue equations to effectively cancel the error.

$V_{tavg}$ is the average of the two true airspeed sensors. When an FD occurs the filter is no longer updated. FD is accomplished by the means discussed in section 6.1.

The airspeed residues are calculated as:

$$V \text{ Residue \#1} = \Sigma(\text{current } V_{t1} \text{ measured} - \text{previous } V_{t1} \text{ measured} - \dot{V}_x \, dt)$$

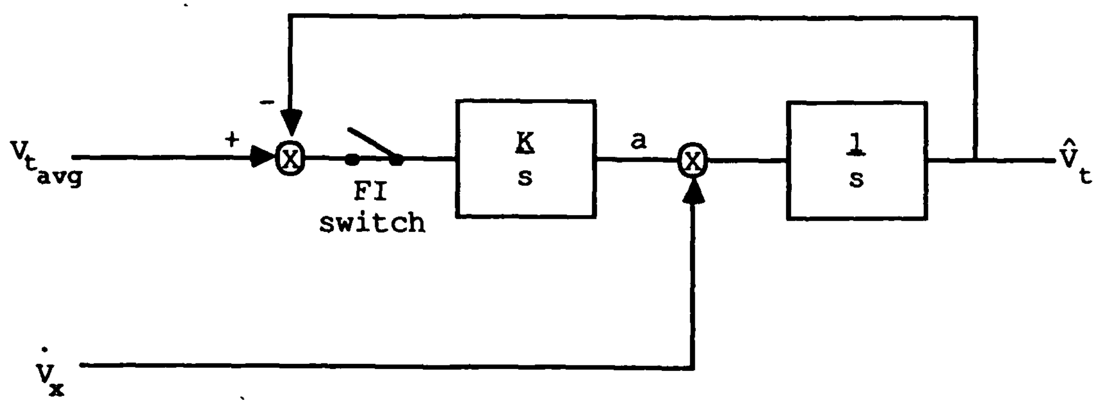
where dt is the update rate. This equation is duplicated for each airspeed sensor measurement. The two residues are then evaluated by an FI algorithm as discussed in section 6.1.

Similar comments concerning error analysis and adaptive threshold solutions apply for this example also. The standard deviation of the average of the sensors could be calculated with a moving window prior to an FD.

### 6.3. Stability Augmentation System

A large number of advanced aircraft are not statically stable. This is a concern because the airframe is no longer inherently stable. As an aircraft's center of gravity moves aft, the wing has a decreasing capacity to generate a nose down moment in response to an increase in angle of attack. At the neutral point, there is no pitch-axis response due to a change in angle of attack. When the center of gravity is farther aft than the neutral point, a pitch-up moment is generated from an increase in angle of attack which may make the aircraft very difficult to fly.

A Relaxed Static Stability (RSS) aircraft requires an SAS to restore stability to reasonable levels. If the SAS function is critical, it makes sense to implement AR rather than to increase the number of sensors. This function is dependent on feedback from inertial sensors, pitch angle, pitch rate, and vertical acceleration, or air data sensors, true airspeed, and angle of attack, to prevent a rapid pitch-axis divergence.



a is an estimate of error on $\dot{V}_x$, subsequently added to each $\dot{V}_x$ calculation in the fault isolation residue equations to effectively cancel the error.

FIGURE 6.2-1. EXAMPLE FILTER USED FOR TRANSLATIONAL KINEMATICS REDUNDANCY

An estimate of pitch rate and vertical acceleration can be determined with the following equations.

$$Q_E = Q_m - \dot{\theta}\cos\varnothing_m + \dot{\tau}\sin\varnothing_m\cos\theta_m$$

$$A_{zE} = A_{zm} - U_m(Q_m - \dot{\alpha}_m) - g\cos\theta_m\cos\varnothing_m \text{ assuming that } V = 0$$

where Q = pitch rate

$A_z$ = vertical acceleration

U = x-axis velocity

g = acceleration due to gravity

Ø = roll angle

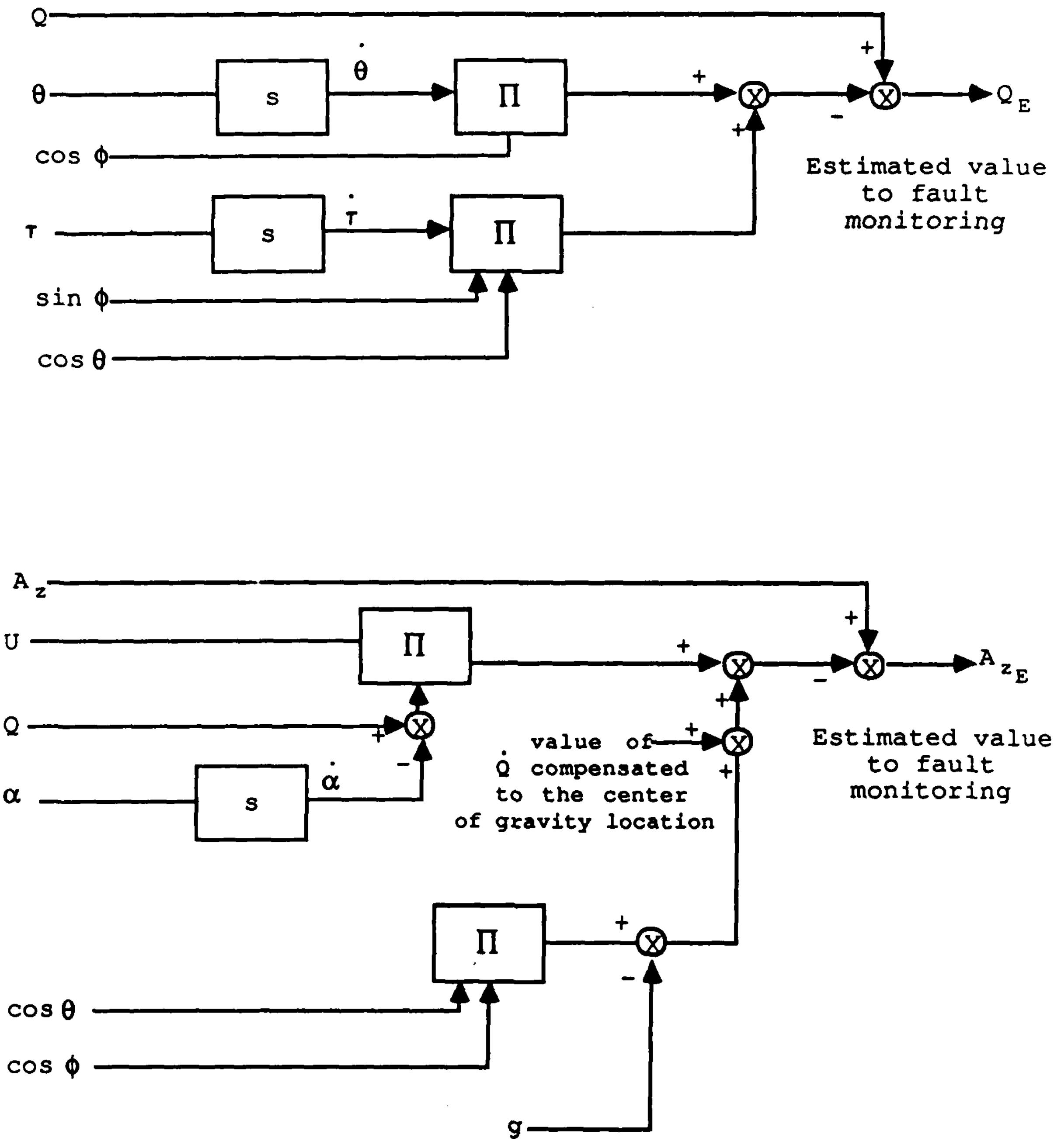
$\theta$ = pitch angle

$\tau$ = yaw angle

$\alpha$ = angle of attack ≈ W/U where W is the vertical velocity.

The subscript m denotes measured quantities and the subscript E denotes an estimated value.

Figure 6.3-1 shows one way to implement filters for these two estimated values. FD and isolation is as described in section 6.1.



Estimated value to fault monitoring

value of $\dot{Q}$ compensated to the center of gravity location

Estimated value to fault monitoring

FIGURE 6.3-1. EXAMPLE FILTERS USED FOR STABILITY AUGMENTATION SYSTEM

# BIBLIOGRAPHY

Athans, M. and D. Willner, "A Practical Scheme for Adaptive Aircraft Flight Control Systems," Symposium on Parameter Estimation Techniques and Applications in Aircraft Flight Testing, NASA Flight Research Center, Edwards Air Force Base, April 24-25, 1973.

Beard, R. V., Failure Accommodation in Linear Systems Through Self-Reorganization, Report MVT-71-1, Man-Vehicle Laboratory, Cambridge, MA, February 1973.

Buxbaum, P. J. and R. A. Haddad, "Recursive Optimal Estimation for a Class of Nongaussian Processes," Proceedings of Symposium on Computer Processing in Communications, Polytech Institute of Brooklyn, April 8-10, 1969.

Chien, T. T., An Adaptive Technique for a Redundant-Sensor Navigation System, Report T-560, Draper Labs, Cambridge, MA, February 1972.

Clark, R. N., et al., "Detecting Instrument Malfunctions in Control Systems," IEEE Transactions on Aerospace and Electronic Systems, Vol. AES-11, No. 4, July 1975.

Cunningham, T., and G. Hartmann, Fault Tolerant Digital Flight Control with Analytical Redundancy, Technical Report AFFDL-TR-77-25, May 1977.

Davis, M. H. A., "The Application of Nonlinear Filtering to Fault Detection in Linear Systems," IEEE Transactions on Automatic Control, Vol. AC-20, No. 2, April 1975.

Deckert, J. C., et al., Reliable Dual- Redundant Sensor Failure Detection and Identification for the NASA F-8 DFBW Aircraft, NASA Contractor Report 2944, February 1978.

Desai, M. N., J. C. Deckert, and J.J. Deyst, "Dual Sensor Failure Identification Using Analytical Redundancy," Journal of Guidance and Control, Vol. 2, No. 3, May-June 1979.

Deyst, J. J. and J. C. Deckert, "RCS Jet Failure Identification for the Space Shuttle," Proceedings of IFAC 1975, Cambridge, MA, August 1975.

Hartmann, G. L., et al., Digital Adaptive F-8C Control Laws, Final Report NAS 1-13358, July 1975.

Jones, H. L., Failure Detection in Linear Systems, PhD Thesis, Department of Aeronautics and Astronautics, MIT, Cambridge, MA, September 1973.

Kaniuka, W. W., et al., *New Flight Control Technologies for Future Naval Aircraft*, Report No. NADC-82240-60, September 1982.

Kerr, T. H., "A Two Ellipsoid Overlap Test for Real-Time Failure Detection and Isolation by Confidence Regions," *IEEE Conference on Decision and Control*, Phoenix, AZ, November 1974.

Lainiotis, D. G., "Joint Detection, Estimation, and System Identification," *Information and Control*, Vol. 19, No. 1, August 1971.

Maybeck, P. S., "Failure Detection Through Functional Redundancy," AFFDL-TR-74-3, January 1974.

McAulay, R. J. and E. Denlinger, "A Decision-Directed Adaptive Tracker," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. AES-9, March 1973.

McGarty, T. P., "State Estimation with Faulty Measurements: An Application of Bayesian Outlier Rejection," *Proceedings of the Fifth Symposium on Nonlinear Estimation and Its Applications*, San Diego, CA, September 1974.

Mehra, R. K. and J. Peschon, "An Innovations Approach to Fault Detection and Diagnosis in Dynamic Systems," *Automatica*, Vol. 7, 1971.

Meier, L., D. W. Ross, and M. B. Glaser, "Evaluation of the Feasibility of Using Internal Redundancy to Detect and Isolate On-Board Control Data Instrumentation Failures," AFFDL-TR-70-172, January 1971.

Montgomery, R. C. and A. K. Caglayan, "A Self-Reorganizing Digital Flight Control System for Aircraft," *AIAA 12th Aerospace Sciences Meeting*, Washington, D.C., January 30-February 1, 1974.

Montgomery, R. C. and D. B. Price, "Management of Analytical Redundancy in Digital Flight Control Systems for Aircraft," *AIAA Mechanics and Control of Flight Conference*, Anaheim, CA, August 5-9, 1974.

Mulcare, D. B., L. E. Downing, and M. K. Smith, *Analytical Sensor Redundancy Assessment*, DOT/FAA/CT-86/32, Draft Report, June 1987.

Pierce, B. D. and D. D. Sworder, "Bayes and Minimax Controllers for a Linear System with Stochastic Jump Parameters," *IEEE Transactions on Automatic Control*, Vol. AC-16, No. 4, August 1971.

Ratner, R. S. and D. G. Luenberger, "Performance-Adaptive Renewal Policies for Linear Systems," *IEEE Transactions on Automatic Control*, Vol. AC-14, No. 4, August 1969.

Ross, S. M., "Introduction to Probability Models," *Academic Press*, 1972.

Sanyal, P. and C. N. Shen, "Bayes' Decision Rule for Rapid Detection and Adaptive Estimation Scheme with Space Applications," *IEEE Transactions on Automatic Control*, Vol. AC-19, June 1974.

Stein, G. and G. L. Hartmann, F-8C Adaptive Control Extensions, NASA Contract NAS 1-13383, June 1976.

Sworder, D. D. and V. G. Robinson, "Feedback Regulators for Jump Parameter Systems with State and Control Dependent Transition Rates," IEEE Transactions on Automatic Control, Vol. AC-18, No. 4, August 1973.

Sworder, D. D., "Bayes' Controllers with Memory for a Linear System with Jump Parameters," IEEE Transactions on Automatic Control, Vol. AC-17, February 1972.

Weinstein, W., Feasibility and Design Studies of an Integrated Sensory Subsystem (ISS) for Advanced V/STOL Aircraft, Report No. NADC-76259-30, March 1978.

Willsky, A. S., J. J. Deyst, and B. S. Crawford, "Adaptive Filtering and Self-Test Methods for Failure Detection and Compensation," Proceedings of the 1974 JACC, Austin, Texas, June 19-21, 1974.

Willsky, A. S. and H. L. Jones, "A Generalized Likelihood Ratio Approach to State Estimation in Linear Systems Subject to Abrupt Changes," Proceedings of the 1974 Conference on Decision and Control, Phoenix, AZ, November 1974.

## GLOSSARY

ANALYTICAL REDUNDANCY. The use of software algorithms which use known mathematical relationships between different sensors for sensor failure detection and replace most of additional redundant sensor hardware.

CONTROL LAW. The physical relationship between various sensors and control surfaces.

COVERAGE. The percent confidence level of a given analytical redundancy fault detection and isolation algorithm for all types of faults.

DIAGNOSTIC FILTER. An analytical algorithm which processes data from N functionally related sensors. The data are used to estimate some sensor outputs and assess the correct functioning of the sensors.

DUAL FAIL-OPERATIONAL. A reliability requirement placed on a system which requires the system to be operational after two failures have occurred.

FAIL-OPERATIONAL. A reliability requirement placed on a system which requires the system to be operational after a single failure has occurred.

FAIL-SAFE. A reliability requirement placed on a system which requires that safe flight not be hindered even after a failure.

FALSE ALARM. The declaration of a fault by a fault detection monitor or algorithm when there is no fault.

FAULT DETECTION. The determination that a sensor is faulted by using a software algorithm.

FAULT ISOLATION. The determination that a particular sensor is faulted by using a software algorithm.

FAULT TOLERANCE. Accommodation of sensor hardware faults based on some type of comparator scheme.

FLIGHT-CRITICAL. A description of functions whose failure would contribute to or cause a failure condition preventing the continued safe flight and landing of the aircraft.

MISSED ALARM. The failure of a fault detection monitor or algorithm to detect a fault when there is a sensor fault.

MULTIPLE TRIP MONITOR. A fault detection algorithm which declares a fault after the sensor output has exceeded a predefined threshold N times.

OBSERVER. An algorithm which models physical relationships between sensor data and uses the data to provide fault detection for one or more sensors. This is also known as a Luenberger observer or a signal blender.

REDUNDANCY MANAGEMENT. The computer processing which is needed to implement fault detection and isolation algorithms.

REVERSION MODE. The high level of redundancy in a system having different redundancies requirements for some sensors. Critical sensors may have a high level of redundancy while other sensors have low levels.

SENSOR. An instrument which measures a particular physical parameter. The data output may be digital or analog and is utilized by the flight computer.

SEQUENTIAL LIKELIHOOD RATIO TEST. A fault detection algorithm which is based on two hypothesized density functions of no fault or sensor fault.

SEQUENTIAL PROBABILITY RATIO TEST. See sequential likelihood ratio test.

SUPER-DIAGNOSTIC FILTER. An algorithm which provides all the capabilities of a diagnostic filter. Additionally, it can isolate a specific faulted sensor. At the current time, this is the most complex technique used to implement analytical redundancy.

## ACRONYMS

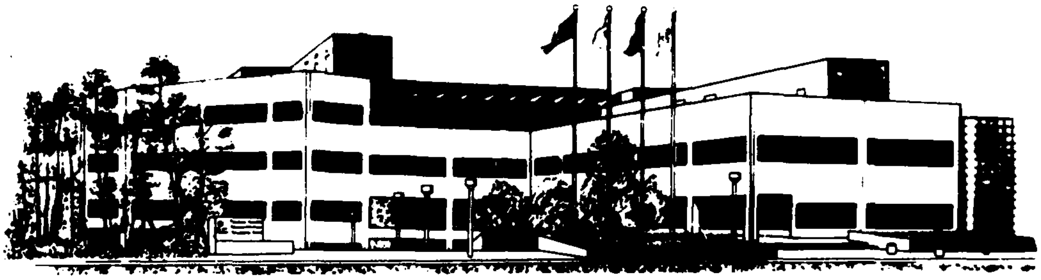
| | |
|---|---|
| AFFDL | Air Force Flight Dynamics Laboratory |
| AK | Altitude Kinematics |
| AR | Analytical Redundancy |
| C | Comparator |
| CARSRA | Computer Aided Redundant System Reliability Analysis |
| DF | Diagnostic Filter |
| DFC | Digital Flight Control |
| DFCS | Digital Flight Control System |
| DOT | Department of Transportation |
| FAA | Federal Aviation Administration |
| FBW | Fly-By-Wire |
| FD | Fault Detection |
| FI | Fault Isolation |
| NADC | Naval Air Development Center |
| NASA | National Aeronautics and Space Administration |
| RM | Redundancy Management |
| RSS | Relaxed Static Stability |
| SAS | Stability Augmentation System |
| SDF | Super-Diagnostic Filter |
| SLRT | Sequential Likelihood Ratio Test |
| SPRT | Sequential Probability Ratio Test |

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 8
## ESTIMATION AND MODELING FOR REAL-TIME SOFTWARE RELIABILITY MODELS



**PREPARED BY:**

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

**PREPARED FOR:**

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

## NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# TABLE OF CONTENTS

## TABLE OF CONTENTS

Section Page

APPENDICES

## TABLE OF CONTENTS

# LIST OF ILLUSTRATIONS

# LIST OF TABLES

Table Page

# 1. INTRODUCTION

## 1.1. What is Software Reliability

Industry concern for software reliability is growing as increasingly complicateᵉᵈ computer software is being used to perform critical tasks. Software reliability is "the probability that a given software program operates for some time period, without a software error, on the machine for which it was designed given that it is used within design limits." (Dickson et al., cited by Gephart et al., 1978, p. 2). A number of methods have been proposed for improving software quality and predicting its reliability. Until recently, software developers assumed that the testing strategy selected would be sufficient to detect all faults or failures in the software prior to its implementation. However, rapid increases in software complexity have made it impossible to thoroughly test the software within the constraints of reasonable time and budget.

There are two possible approaches to the problem of software reliability. The first approach is to use reliability models that predict the number of software faults expected and the likelihood that these faults will cause a system failure. Such predictions are based upon data acquired through initial testing of the software. This information can then be used to guide the testing process and to provide a reliability confidence level. The objective of this approach is to find and remove all faults in the software. Fault-intolerant (or single-version software) is software to which these models can be applied.

A second approach assumes that software faults are likely to occur. Finding each fault, however, may not be possible. Rather than attempting to remove all faults, this approach tries to develop safeguards within the software that will support recovery from software failures or at least minimize the consequences of such failures. Reliability models have been developed in response to such fault-tolerant software. These models are used to predict the reliability of this type of software and to determine the types and number of safeguards that need to be included in a given type of software. Fault-tolerant reliability models are used even before the software has been coded. Consequently, results from the application of these models can guide the subsequent design and development of the actual software. This tutorial looks at both fault-tolerant and fault-intolerant reliability models that are appropriate for use with complex real-time software such as that used in avionics and flight control systems.

## 1.2. The Scope of this Tutorial

This tutorial provides aircraft certification specialists with the background needed to understand and evaluate documents that describe measures taken to assess software reliability submitted as part of the certification process for advanced digital avionics and flight control systems. It should be noted, however, that the development of software reliability methodologies is still in its infancy. As a result, there is little agreement as to how and when these models should be applied, and which models are most appropriate for specific use situations. The reader who seeks hard and fast rules will be disappointed to discover that such rules simply do not exist. Consequently, this tutorial can only present the concept of reliability models, define their processes and goals, and describe those models which are considered acceptable and likely to be applied.

The unquestionable need for such models necessitates their use even though questions of theory and application remain. Specific guidelines and recommendations which can be directly applied to evaluating certification documents remains a future objective.

This tutorial is divided into five major sections:

- "Introduction" and "Topic History" provide overviews of software reliability: Why it is used and what it tries to accomplish. Two broad categories of software reliability models are also introduced.

- "The Software Development Process" briefly describes the stages involved in software development, the opportunities for faults to be introduced into the software, and limitations in current testing approaches intended to remove faults. This section is intended to serve as a framework for understanding when reliability models are used and how they compare with some existing approaches to supporting high software quality.

- "Fault-intolerant Software Reliability Models" looks at reliability models which are used with real-time, single-version or fault-intolerant software.

- "Fault-tolerant Reliability Models" addresses reliability models designed specifically for use with fault-tolerant software.

- The appendices contain worked examples demonstrating how the most important models (representing both the fault-tolerant and fault-intolerant categories) are used. Following the appendices are supplemental materials, including references, which can serve as a basis for further study in this area, and a glossary of terms.

# 2. TOPIC HISTORY

## 2.1. Introduction

Traditionally, improvements in aircraft design have been aimed at more efficient aerodynamic designs and propulsion systems (Larsen, et al., 1984). Recently, however, the greatest advancements have been in the development of digital electronic systems and devices for flight control and avionics systems. Examples of such systems include stability and control augmentation systems, active control systems, advanced displays, aircraft/crew interface, and aircraft handling and gust-load alleviation systems. Such systems rely on extensive software to monitor their functioning and maintain appropriate system conditions. With this growing emphasis on critical software functioning comes the requirement for methods to evaluate the reliability of this software.

Although reliable software is important for all applications, it is imperative for flight-critical software. Since in-use software testing of flight-critical systems is not a safe option, other methods must be implemented to demonstrate that the software can be relied upon to perform its intended function.

Hardware reliability assessment has been in use for more than 20 years. Hardware reliability models and procedures have proved useful and have achieved acceptance as validation tools. Although software reliability assessment has been around almost as long - 15 years - acceptance within the industry has been slow. Acceptance and implementation are expected to improve for many reasons, including:

- The recognition of a growing reliance on software to perform critical tasks. (A trend that is likely to continue.)

- The increasing use of software to perform tasks traditionally performed by hardware.

- The increased software development and operational costs compared to hardware costs.

Computer hardware costs are closely linked to technological advances in integrated circuit technology. Hardware advances pose a challenge to the software designer to develop software that will effectively utilize complex, innovative hardware. The complexity of such software has outgrown the technology for designing and testing it. Workable reliability assessment methods are therefore critical.

As figure 2.1-1 (Shooman, 1984) shows, hardware manufacturing costs have been decreasing over the past 30 years as hardware technology advances. Software costs, however, continue to increase.

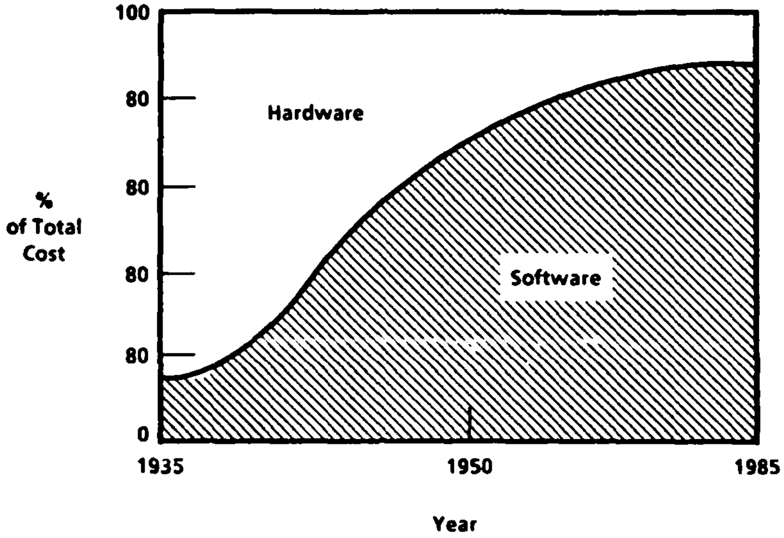


FIGURE 2.1-1. HARDWARE AND SOFTWARE COST TRENDS (from Shooman, 1984)

Software costs are roughly proportional to the number of lines of code in the program. Consequently, greater software complexity is accompanied by higher labor costs. Greater complexity also increases the likelihood of errors being made in the design and coding of software. Not surprisingly, the bulk of software development costs are devoted to testing and validation, a cost which also grows with increases in software complexity.

Concerns with software reliability can be traced back to two pressures: The need to reduce development costs, with the testing and validation stage as a major target; and the increasing likelihood of errors due to more complex software.

Attempts to reduce software errors conflict with attempts to reduce software costs. Obvious ways of reducing errors include devoting more time to the early stages of software design, such as development of software specifications and requirements (to enhance software quality) and thorough testing of the software. Both approaches are labor intensive and extremely costly, and can have a major impact on software development time. Therefore, there is a need to find other methods which promise effective but less expensive solutions.

Two approaches to offering more cost-effective quality control are described in this tutorial. The first approach is single-version software reliability modeling. The second approach is the development of fault-tolerant software.

- Single-version software reliability modeling serves two important functions (Goel, 1983). The modeling provides (1) a useful decision tool for software development planning, and (2) some assurance of how well the software can be expected to perform over time.

Based upon the results of these models, educated decisions can be made concerning how staff time and other costs can be allocated to produce the highest quality software. Predictions of the number of remaining faults enable software developers to determine the additional costs required for incremental enhancements in software reliability.

The cost of finding remaining faults rises very quickly. As faults are removed, remaining faults become more difficult to locate. At some point removing additional faults is no longer cost effective. Justification for decisions about reasonable reliability levels can be based, in part, on objective measures (i.e., performance parameters) provided by software reliability models.

- Fault-tolerant software has safeguards built into the software to enable it to detect and recover from faults, avoiding system failures or minimizing their impact.

  Examples of these safeguards include N-version Software (NVS) and Recovery Block (RB) methodology. NVS refers to incorporating multiple versions of the same software module, which have been developed by different coders, into the software program. When one version fails, a second version can be tried. The process continues until a version is successfully run.

  The RB method refers to providing components which may be alternated with a faulty component. Software reliability models have also been developed for fault-tolerant software. Such models provide the same benefits as single-version reliability models. Results of these models can be used for software development planning and assurance of software reliability.

## 2.2. Achieving System Reliability Estimates

Software reliability models attempt to achieve the same objectives as their hardware reliability counterparts: To provide reliability estimates that can contribute to estimation of overall system reliability. Initial attempts at software reliability modeling were based upon hardware reliability constructs. However, inherent differences between hardware and software have resulted in software reliability models assuming a somewhat different approach. This is especially true for single-version, fault-intolerant software models.

Hardware reliability models are developed on the basis of known failure rates for the components or modules comprising the system. These failure rates can be estimated using known values from Department of Defense (DOD) MIL-HDBK-217 or relying on past experience with similar hardware components. In the case of software reliability estimation, there are no failure rate standards. Although software is constructed by integrating existing pieces or modules into a newly integrated package, fault data do not exist for these entities.

There are other differences between software and hardware which prevent the simple application of hardware models to software estimation. A major difference lies in the source of faults. In the case of hardware, faults are introduced during the manufacturing stage, when each individual module is built. Each time a module is manufactured, there is a possibility that faults in the parts or parts or entire assemblage may result. Faults may also appear during use as the module ages and wears. In contrast, software faults occur primarily during the design and development process. Copying the software does not produce new faults or wear out the software.

The primary consequence of these differences can be seen in failure rate curves viewed over the life cycle of the system. Hardware failures will start high and then drop as the faults are fixed. The failure rate will then remain constant until modules begin to wear out, at which time the failure rate will begin to increase again. Software, in contrast, will start high and drop, achieving a similar constant failure rate as is found in hardware. However, there will not be a subsequent increase over time since the software does not wear out. Consequently, software exhibits reliability growth. Other differences between hardware and software are summarized in table 2.2-1 (Krauson and Baker, 1982).

TABLE 2.2-1. COMPARISON OF HARDWARE AND SOFTWARE PROPERTIES (from Krauson and Baker, 1982)

| | Characteristic | |
|---|---|---|
| Property | Hardware | Software |
| Ratio of Errors | Errors cause a relatively large (60% to 80%) portion of system failures | Errors cause a relatively small (20% to 40%) but significant portion of system failures |
| Parts Interchangeability | Many components are identical | Each module has a unique function and implementation |
| Fault Replication | Different copies of identical components have different defects | All copies of the same master have the same faults |
| Usage | Usage causes wear defects | Usage has no effect on faults |

In the past, the inability to apply hardware reliability models to software has resulted in the assumption that software reliability has a value of 1.0. This value was then used to compute system reliability. In recent years, the increasingly critical role of software in overall system performance has made this assumption untenable. Software reliability must be either obtained from exhaustive testing or estimated, rather than assumed, in order to properly assess system reliability.

These differences have affected the development of fault-intolerant and fault-tolerant software reliability models in unique ways. Assessment of single-version, fault-intolerant software reliability involves predicting the expected number of faults in the software as a whole. Since there are no a priori standards for expected number of faults, as are available for hardware, an initial testing phase must take place. Based upon the number of faults detected during testing, statistical methods can then be used to predict the fault distribution and estimate the remaining number of errors. Testing can then continue, if required, until remaining faults are found and corrected.

Fault-tolerant reliability methods are more similar to hardware methods. Within fault-tolerant software systems are individual software modules, such as each of the multiple versions of a given software module (NVS), RBs, and other "pieces." These pieces are conceptually similar to individual hardware modules. The similarity ends here in that currently there are no fault standards for these individual software modules. Rather, reliability for these modules must be estimated using testing and other procedures. Ideally, a database, which will include module reliability data, will be compiled over the next five to ten years as more experience is gained using these techniques. Overall software reliability is then determined through combining individual module reliabilities, as is the case with hardware.

# 3. THE SOFTWARE DEVELOPMENT PROCESS

## 3.1. Relationship Between the Software Development Process and Software Reliability Estimation

Gephart et al., 1978 have developed a generic model of software error rate as a function of software life cycle. Figure 3.1-1 (Gephart et al., 1978) shows how error rate varies with the phase of the software development cycle. Phase I, the design and initial test'ng period, involves designing equations and algorithms; preparing flowcharts; and writing, testing, and integrating individual software modules. Types of errors likely to occur during this phase include typographical errors, syntax errors, and logic errors. Typically, initial system integration testing is performed at the end of this phase.

"Advanced" testing, involving the program as a whole, takes place during the second phase, and includes subjecting the software to inputs thought to be typical of the use environment. By the end of this phase, the software is actually fielded. Phase III, an operational phase, involves only limited maintenance. Two types of errors will be removed in Phase III: (1) Those which have critical impact on system performance, and (2) Those whose removal is cost-effective. Phase IV involves operational use and, typically, no maintenance is performed.

Because Phase I is the design phase, the error rate is likely to be quite high and perhaps erratic. As the software becomes more structured and integrated, and extensive testing is performed, error rates will become more predictable and show a declining rate during Phase II as testing and debugging efforts continue. During Phase III, the error rate will continue to decline, eventually leveling off. Typically, error data used for reliability assessment are acquired during Phases II and III, allowing identification of error distributions and predicting the expected number of errors. The accuracy of reliability assessment depends, not surprisingly, on the quality of the error data obtained during these phases.

Since most of the errors have been identified and corrected during the first three phases, Phase IV errors tend to be infrequent and occur as a function of using a previously untested path as a result of an unanticipated situation. These errors are difficult if not impossible to find and correct. Some errors are never corrected, because they cannot be found within the constraints of reasonable time and cost. Also, an error may not always be successfully corrected, and the process of correcting one error may introduce new errors. Therefore, the error rate in Phase IV tends to be constant and mostly nonexistent.

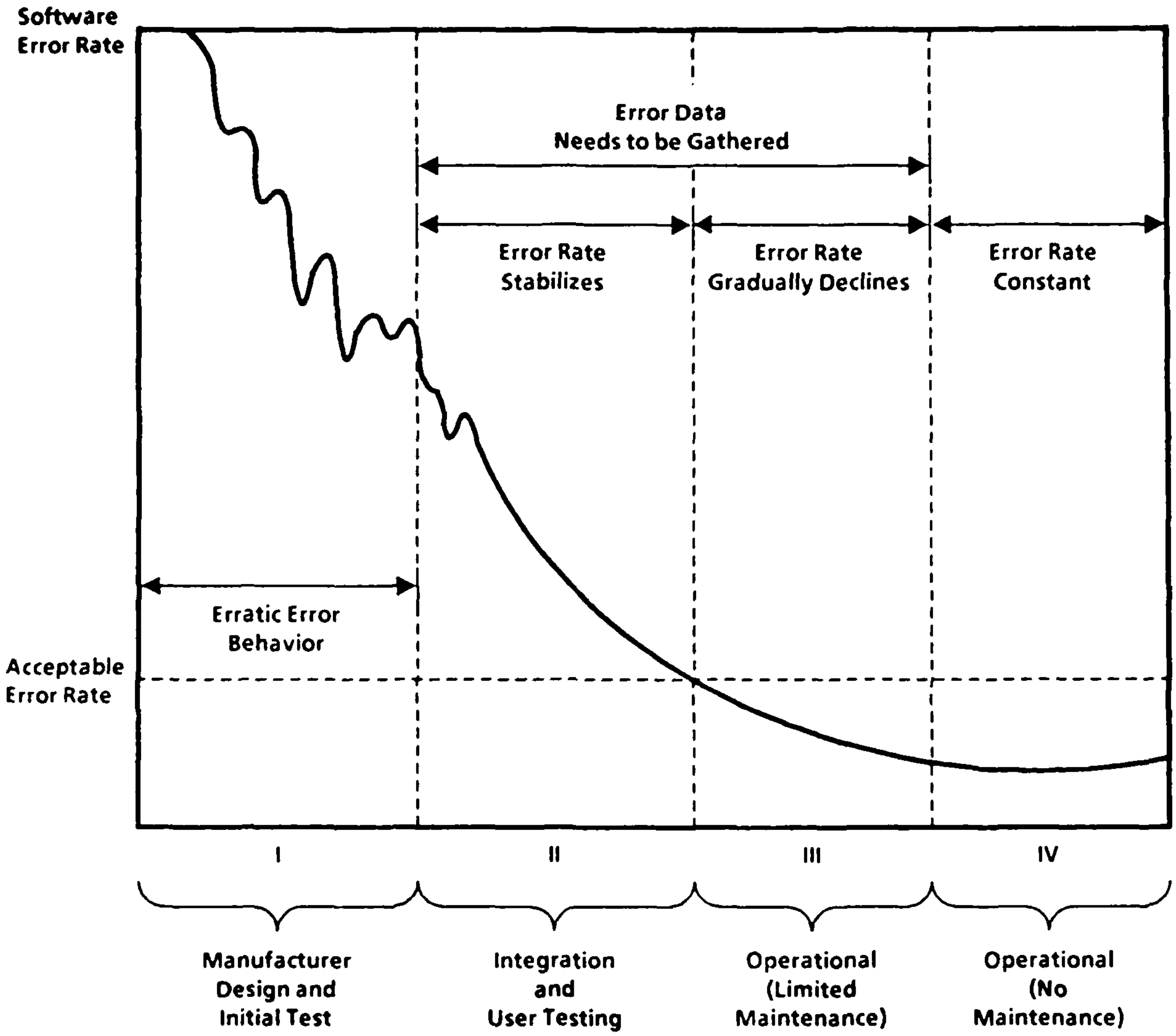


FIGURE 3.1-1. PHASES OF SOFTWARE DEVELOPMENT
(Gephart et al., 1978)

## 3.2. Software Testing

Software testing, used primarily during Phases II and III to determine the existence of errors in the coded software, is a somewhat heuristic process: Testing effectiveness is dependent upon the tester's ability to define test selection rules which, in turn, can be translated into tests that are sufficient for verifying the software's correctness. Test cases can be generated based upon the structure of the software (statements, control flow, etc.) or the functions identified in the functional specification. In either case, testing will reveal the presence of only those errors it was designed to identify; it will not detect those errors which are outside the testing boundaries.

A potential solution to this problem is the development of a metric (or methodology) which can be used to predict (based on data obtained during testing) the overall reliability of the software, including the expected number of errors in the program. This is the approach taken by software reliability models which have been specifically developed to address these problems. It is the subject of the next portion of this tutorial.

# 4. FAULT-INTOLERANT RELIABILITY MODELS

## 4.1. Introduction

In this section, the assumptions and characteristics of one category of software reliability models, those designed for single-version, fault-intolerant software, are presented. These models, which are based mainly on the failure history of the software, are time-dependent. The time-dependent approach uses either the times between failures (time-between-failure models) or the number of failures observed in a sequence of test time intervals (error-count models) to estimate the reliability of the software undergoing testing.

Both classes of time-dependent models are intended to be used during the software testing and debugging phase to provide either a reliability estimate or some other useful parameter (e.g., number of remaining errors, test reliability, and confidence in the program) which in turn yields some measure of the correctness of the program. Application of these models relies on methods of testing, verification, code walk-through, etc. to first provide the raw data (either as time between failures or as number of failures per individual test interval). Models are then used to estimate the expected performance statistics based on the use of maximum likelihood estimation (or least squares approximation) statistics and the underlying distribution of the data. This process, based on Goel's (1983) description and example data, is explained in more detail below and is summarized in figure 4.1-1.

### 4.1.1. Step 1: Evaluating the Failure Data Acquired From Testing

The initial step in selecting and applying a reliability model is to examine the test error data in order to identify the underlying data distribution. Identification of the data distribution is crucial because this distribution determines (1) whether the data can appropriately be modeled by time-dependent models; and (2) which class of time-dependent models (time-between-failure or failure-count) should be used. To ensure that the actual data distribution is attained, biases in the testing process need to be accounted for in the modeling process. For example, the actual distribution may be distorted if more and more functions were added during the subsystem or system test, or if test case severity changed during testing. Such biases may be compensated for by use of statistical procedures, such as normalizing the data to meet the steady-state system assumption of the models.

To demonstrate how the reliability modeling process occurs, an example will be shown. The data to be used are given as times between failures and are shown in table 4.1-1 (Goel, 1983). These data are also plotted in figure 4.1-2 (Goel, 1983).

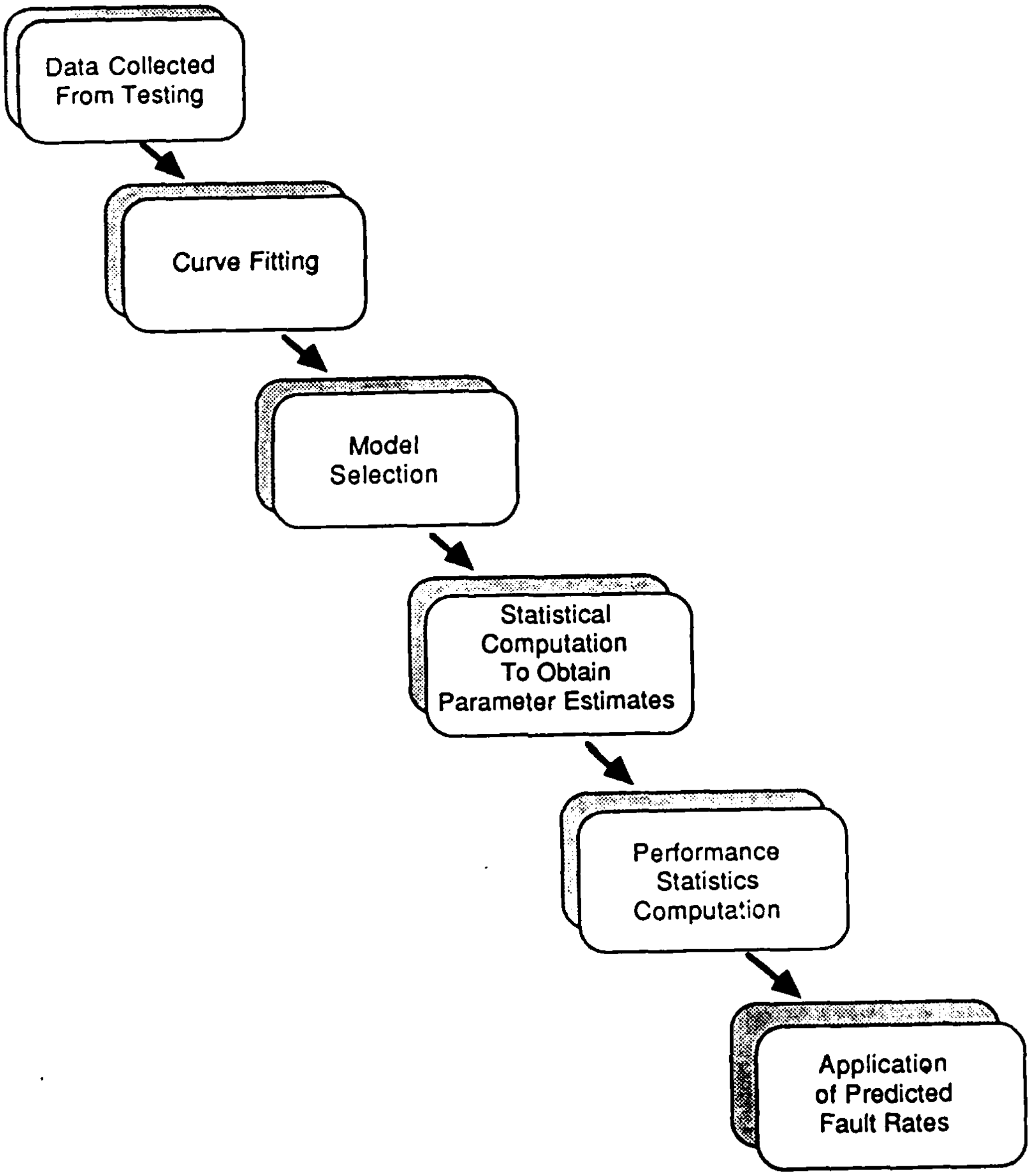

Data Collected From Testing
Curve Fitting
Model Selection
Statistical Computation To Obtain Parameter Estimates
Performance Statistics Computation
Application of Predicted Fault Rates

FIGURE 4.1-1. FLOW FOR COMPLETING THE SOFTWARE RELIABILITY ESTIMATION PROCESS

TABLE 4.1-1. FAILURES IN ONE HOUR (EXECUTION TIME) INTERVALS AND CUMULATIVE FAILURES (from Goel, 1983)

| Hour | No. | Cum. |
|---|---|---|
| 1 | 27 | 27 |
| 2 | 16 | 43 |
| 3 | 11 | 54 |
| 4 | 10 | 64 |
| 5 | 11 | 75 |
| 6 | 7 | 82 |
| 7 | 2 | 84 |
| 8 | 5 | 89 |
| 9 | 3 | 92 |
| 10 | 1 | 93 |
| 11 | 4 | 97 |
| 12 | 7 | 104 |
| 13 | 2 | 106 |
| 14 | 5 | 111 |
| 15 | 5 | 116 |
| 16 | 6 | 122 |
| 17 | 0 | 122 |
| 18 | 5 | 127 |
| 19 | 1 | 128 |
| 20 | 1 | 129 |
| 21 | 2 | 131 |
| 22 | 1 | 132 |
| 23 | 2 | 134 |
| 24 | 1 | 135 |
| 25 | 1 | 136 |

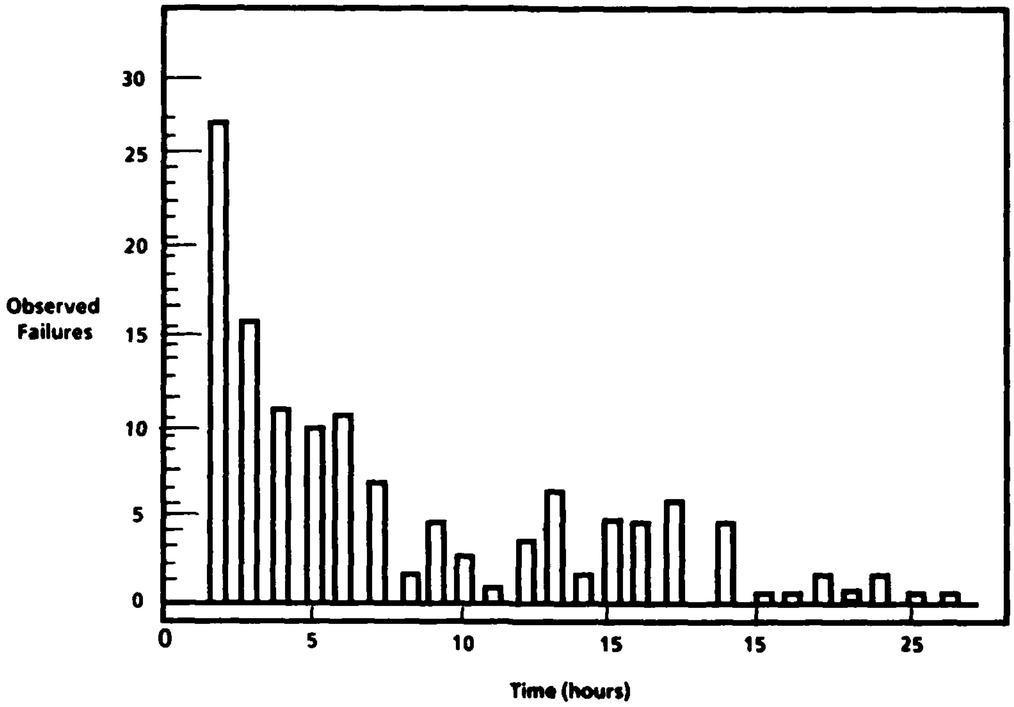


FIGURE 4.1-2. OBSERVED FAILURES PER HOUR (from Goel, 1983)

## 4.1.2. Step 2: Curve Fitting

After the data have been plotted, examined, and normalized (as required), decisions about the applicability of a class of models or the selection of a specific model can be made based upon the apparent distribution of the data. The two classes of models (time-between-failure, failure count) require different assumptions, as outlined in table 4.1-2. In addition, each class of model assumes a specific statistical distribution.

In the case of time-between-failure models, the test data must follow an exponential distribution since these models assume that the failure interval is constant and proportional to the current fault content of the program. The constant failure rate assumption means that for a given system of software, a given failure can be expected to occur during the next time interval regardless of when during testing the time interval is selected. However, successive times between failure are expected to increase in duration as faults are removed from the software. (Note that for a given set of test data this may not be entirely true, since the failure times are random variables and the resultant data are subject to statistical fluctuations.) Thus, for this given class of models, the assumed underlying distribution is expected to reflect the overall improvement in software quality as faults are detected and removed. The parameters of the distribution depend upon the number of faults remaining in the system, in a given interval, after the ith failure.

TABLE 4.1-2. FAULT-INTOLERANT SOFTWARE RELIABILITY MODEL ASSUMPTIONS (*from Goel, 1983*)

| Time-Between-Failure Models | Error-Count Models |
|---|---|
| • Independent times between failures | • Testing intervals are independent of each other |
| • Equal probability of the exposure of each fault | • Testing during intervals reasonably homogeneous |
| • Embedded faults are independent of each other | • Numbers of faults detected during non-overlapping intervals are independent of each other |
| • Immediate fault removal, perfect fault removal, no new faults introduced during correction | |

Failure count models attempt to model the number of failures in a given testing interval. As faults are removed from the system, these models assume that the number of failures observed per unit time will decrease and the curve representing cumulative number of failures versus time will eventually level off. Typically, duration of time intervals is fixed a priori and the number of failures in each interval is a random variable. Consequently, the underlying data must be distributed as a poisson distribution in that the failure rate (number of failures per unit time) is expected to decrease over time, thus demonstrating an increase in program reliability.

The data used in the example demonstrate a monotonically decreasing failure rate (number of failures per hour) and appear to conform to a poisson distribution (see figure 4.1-3; Goel, 1983). Consequently, a fault-count model is appropriate for these data.

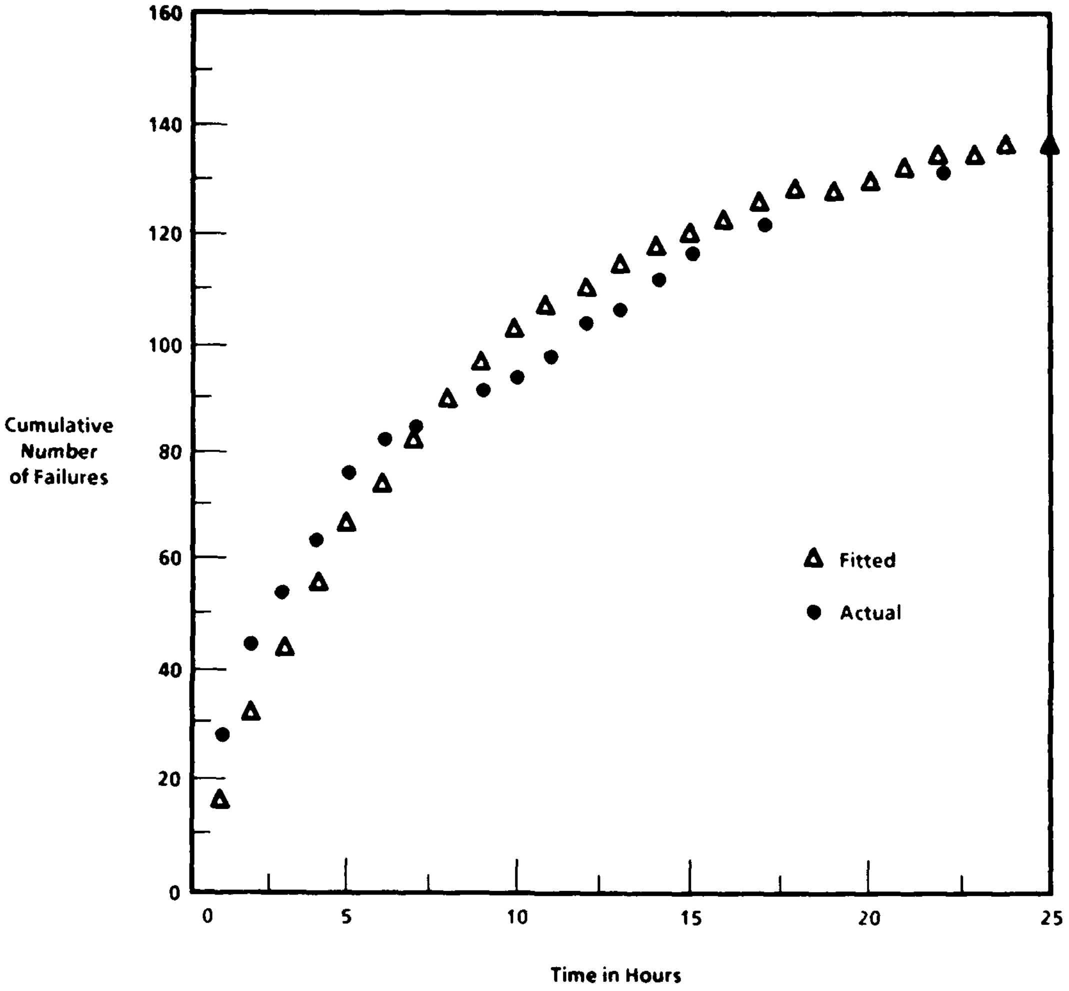


FIGURE 4.1-3. ACTUAL VERSUS PREDICTED FAILURES PER HOUR (from Goel, 1983)

### 4.1.3. Step 3: Model Selection

At this point, a specific fault-count model can be selected based upon the results obtained from the previous two steps. Listed in table 4.1-3 (Goel, 1983) are current time-dependent models appropriate for real-time applications (See Prater, Hitt, and Eldredge, 1986, for a discussion of model requirements for real-time applications.) Included are both time-between-failure and failure-count models.

TABLE 4.1-3. FAULT-INTOLERANT SOFTWARE RELIABILITY MODELS (from Goel, 1983)

| Time-Between-Failure Models | Error-Count Models |
|---|---|
| • Jelinski-Moranda De-Eutrophication Model | • Goel-Okumoto Non-Homogeneous Poisson Process (NHPP) Model |
| • Geometric De-Eutrophication | • Geometric Poisson Model |
| • Generalized Imperfect Debugging Model | • Extended Jelinski-Moranda Model |
| • Bug-Proportional Model | • Modified Geometric De-Eutrophication Model |
| | • Shooman Exponential Model |

Selection of an appropriate model requires that the assumptions of the model be met by characteristics of the data. These assumptions are listed for each model in appendices A and B. (Goel, 1983, provides a useful discussion of the validity of these assumptions.)

For the current example, it was determined that the assumptions associated with the Goel-Okumoto model best corresponded to the data. The assumptions for this model are listed in table 4.1-4.

### 4.1.4. Step 4: Statistical Computation to Obtain Parameter Estimates (from Goel, 1983)

Shown in tables 4.1-5 and 4.1-6 are the various parameters and equations required for reliability estimation for each of the models. The parameters are used by the model to define the shape of the predicted fault distribution and to calculate the performance parameters (such as expected number of errors and expected time to the nth failure) which are given by the equations.

TABLE 4.1-4. ASSUMPTIONS FOR THE GOEL-OKUMOTO NON-HOMOGENEOUS POISSON PROCESS MODEL (from Goel, 1983)

- Initial fault content:

  Expected number of software faults to be eventually detected is an unknown fixed quantity.

  Actual number of faults to be observed is a random variable.

- Independence of faults:

  Each failure is caused by one fault and each of them is equally likely to cause a failure during testing.

  Number of software faults detected during non-overlapping testing intervals is independent of each other.

- Fault removal process:

  Fault removal time is negligible.

  No new faults are introduced during the fault removal process.

- Intensity function:

  Expected number of software faults detected during $(t, t + \Delta t)$ is proportional to the expected number of software faults undetected by time t, i.e.,

  EQN 20

  where

  m(t) = expected number of software faults detected by time t,

  a = expected number of software faults to be eventually detected,

  b = constant of proportionality.

  The intensity function or the fault-detection rate $\lambda(t)$ is a decreasing function of t and is given by

  EQN 21

  where a, b, and m(t) are as defined above.

TABLE 4.1-5. PERFORMANCE MEASURES FOR TIME-BETWEEN-FAILURE MODELS

| Model | Hazard Function | Reliability Function | Mean Time to Failure |
|---|---|---|---|
| Jelinski-Moranda De-Eutrophication Model | $Z(X_i) = \phi[N - (i - 1)]$<br>where<br>N = the total number of initial errors in the program<br>$\phi$ = a proportionality constant<br>$X_i$ = the length of the ith debugging interval (the time between detection of the (i - 1)st and the ith errors)<br>i = the number of errors discovered | $R(X_i) = \exp[-\phi(N-n)X_i]$ | $MTTF = 1/[\phi(N - n)]$<br>where<br>n = the number of errors found to date |
| Geometric De-Eutrophication Model | $Z(X_i) = DK^{i-1}$<br>where<br>$X_i$ = the ith debugging interval<br>D = the initial error detection rate<br>K = a proportionality constant<br>i = the number of errors discovered after i interval | $R(Xi) = \exp[-DK^n X_i]$<br>where<br>n = the total number of errors discovered | $MTTF = \frac{1}{DK^n}$ |
| Generalized Imperfect Debugging Model | $\lambda(t) = \phi(N - p(i - 1))t^{\alpha - 1}$<br>where<br>$\phi$ = a proportionality constant<br>N = the total number of errors<br>p = the probability of perfect programmer debugging behavior<br>$\alpha$ = the parameter that controls the shape of the failure rate | $R(t) = \exp(- \frac{\phi(N - p(i - 1))}{\alpha})t^{\alpha}$ | $MTTF = \frac{1}{\alpha}(\frac{\alpha}{(N - p(i - 1))})^{\frac{1}{\alpha}} \Gamma(\frac{1}{\alpha})$ |
| Bug-Proportional Model | $Z(t) = K\varepsilon_r(\tau) = K[(E_T/I_T) - \varepsilon_c(\tau)]$<br>where<br>K = an arbitrary constant<br>$\varepsilon_r(\tau)$ = the number of remaining bugs<br>$E_T$ = the total number of errors originally present<br>$I_T$ = the total number of machine instructions<br>$\varepsilon_c(\tau)$ = the number of corrected bugs | $R(t) = \exp\{-[K\varepsilon_r(\tau)]t\}$<br>$= \exp\{-K[(E_T/I_T) - \varepsilon_c(\tau)]t\}$ | $MTTF = \frac{1}{K\varepsilon_r(\tau)} = \frac{1}{\beta(1 - \alpha\tau)}$<br>where<br>$\beta = \frac{E_T}{I_T} K$<br>$\alpha = \frac{\rho_O I_T}{E_T}$<br>where<br>$\rho_O$ = a constant rate of error correction |

# TABLE 4.1-6. PERFORMANCE MEASURES FOR FAULT-COUNT MODELS

| Model | Hazard Function | Reliability Function | Mean Time to Failure |
|---|---|---|---|
| Geometric Poisson Model | $Z(t_i) = \lambda K^{i-1}$<br>where<br>$t_i$ = the ith debugging interval<br>$\lambda$ = the average number of faults occurring in the first interval<br>K = a proportionality constant, $0 < K < 1$ | $R(t) = e^{-\lambda K^i t}$ | $MTTF = \frac{1}{\lambda K^i}$ |
| Extended Jelinski-Moranda Model | $Z(t_i) = \phi[N - n_{i-1}]$<br>where<br>$\phi$ = a proportionality constant<br>N = the total number of initial errors<br>$n_i$ = the cumulative number of errors found through the ith time interval<br>$t_i$ = the ith debugging interval | $R(t) = e^{-\phi(N - n_i)t}$ | $MTTF = \frac{1}{\phi(N - n_i)}$ |
| Modified Geometric De-Eutrophication Model | $Z(t_i) = DK^{M_{i-1}}$<br>where<br>D = the fault detection rate<br>K = a positive constant less than 1<br>$M_{i-1}$ = the cumulative number of errors detected<br>$M_i$ = the cumulative number of errors found up to the ith time interval | $R(t) = e^{-DK^{M_n}t}$ | $MTTF = \frac{1}{DK^{M_n}}$<br>where<br>n = the total number of time intervals |
| Shooman Exponential Model | $Z(t) = Ce_r(\tau)$<br>where<br>C = a proportionality constant | $R(t) = \exp\{-C[(E/I) - e_c(\tau)]t\}$<br>where<br>E = the total number of errors present at time $\tau = 0$<br>I = the total number of machine instructions<br>$e_c(\tau)$ = the total number of errors corrected in interval $\tau$ | $MTTF = 1/\{[C(E/I) - e_c(\tau)]\}$ |

| Model | Expected Number of Detected Faults | Expected Number of Remaining Faults | Software Reliability |
|---|---|---|---|
| Goel-Okumoto Non-Homogeneous Poisson Process Model | $\hat{m}(t) = \hat{a}(1 - e^{-\hat{b}t})$ | $E[\hat{\bar{N}}(t)] = \hat{a}e^{-\hat{b}t}$<br>where<br>$\bar{N}(t)$ = *number of faults remaining in the system at time t* | $\hat{R}_{X_k}(S_{k-1}(X\|S) = \exp\{-\hat{a}[e^{-\hat{b}s} - e^{-\hat{b}(s+x)}]\}$<br>where<br>$X_k$ = the time between failures (k - 1) and k<br>$S_k$ = *the time to k failures* |

In order to obtain the parameter estimates, statistical methods (such as least squares and maximum likelihood estimation) are used. In the case of the Goel-Okumoto model, the method of maximum likelihood estimation is used. This statistic provides an estimate of the likelihood that the sample of error data collected during testing actually represents the true data. This is necessary because testing is based on a selected testing strategy that does not thoroughly test all aspects of the software. Consequently, the error data identified is only a subset of the total error data population and may be subject to testing bias.

The basic formula for the Goel-Okumoto model is:

$$m(t) = a(1 - e^{-bt})$$

where a and b are defined as in table 4.1-4.

The total number of software faults detected by time t, N(t), under the above assumptions is representative of the NHPP with mean value functions m(t) and intensity function $\lambda(t)$ as given above. The distribution of N(t), hence, is given by

$$P\{N(t) = y\} = \frac{\{m(t)\}^y}{y!} e^{-m(t)}, y = 0,1,2,\ldots$$

and

$$E[N(t)] = m(t) = a(1 - e^{-bt}) .$$

Using this equation and the method of maximum likelihood estimation as follows, estimates of a and b can oe obtained.

Suppose $y_1, y_2, \ldots, y_n$ are the cumulative number of software faults detected by times $t_1, t_2, \ldots, t_n$, respectively. Then the likelihood function for (a,b) given the data pairs

$$\{(y_i, t_i), i = 1,2,\ldots,n\} \text{ is}$$

$$L(a,b \mid y_1, y_2, \ldots, y_n, t_1, t_2, \ldots, t_n) =$$

$$= \Pr\{N(t_1) = y_1, N(t_2) = y_2, \ldots, N(t_n) = y_n\}$$

$$= \prod_{i=1}^{n} \frac{[m(t_i) - m(t_{i-1})]^{y_i - y_{i-1}}}{(y_i - y_{i-1})!} e^{-\{m(t_i) - m(t_{i-1})\}}$$

$$= \prod_{i=1}^{n} \frac{\{a(e^{-bt_{i-1}} - e^{-bt_i})\}^{y_i - y_{i-1}}}{(y_i - y_{i-1})!} e^{-a(1 - e^{-bt_n})}$$

Maximum likelihood estimation of parameters a and b can then be obtained by solving the following pair of equations simultaneously:

$$a(1 - e^{-bt_n}) = y_n$$

and

$$at_n e^{-bt_n} = \sum_{i=1}^{n} \frac{(y_i - y_{i-1})(t_i e^{-bt_i} - t_{i-1} e^{-bt_{i-1}})}{e^{-bt_{i-1}} - e^{-bt_i}}$$

The above two equations yield

$$\frac{y_n t_n e^{-bt_n}}{(1 - e^{-bt_n})} = \sum_{i=1}^{n} \frac{(y_i - y_{i-1})(t_i e^{-bt_i} - t_{i-1} e^{-bt_{i-1}})}{e^{-bt_{i-1}} - e^{-bt_i}}$$

from which we can find $\hat{b}$ numerically and hence

$$a = \frac{y_n}{(1 - e^{-bt_n})}$$

$\hat{a}$ - 142.32 (Expected number of faults)

$\hat{b}$ - 0.1246 (Faults per fault per hour)

### 4.1.5. Step 5: Computation of Performance Statistics

Tables 4.1-5 and 4.1-6 show the equations used to calculate the performance statistics associated with each model. These performance statistics include: the hazard function, reliability function, and Mean Time to Failure (MTTF). The hazard function estimates the likelihood of software failure at a given instant of time. The reliability function provides an estimate of the probability that the software will not fail in a given time interval. MTTF is the expected value of the time to next failure.

The Goel-Okumoto model uses slightly different performance statistics which are roughly analogous to the performance statistics just described. Computation of these statistics is shown below:

Expected number of software faults detected by time t is given by

$$m(t) = a(1 - e^{-bt})$$

Expected number of remaining faults in the software system at time t is given by

$$E[N(t)] = ae^{-bt}$$

where $\hat{N}(t)$ = number of faults remaining in the system at time t.

Let $X_k$ be the time between failures (k-1) and k and let $S_k$ be the time to k failures. Then it can be shown that the conditional reliability function of $X_k$, given $S_{k-1}$ = s, is,

$$R_{X_k | S_{k-1}}(x | s) = \exp[-a\{e^{-bs} - e^{-b(s+x)}\}].$$

The fitted model is obtained by substituting the above estimated values.

$$\hat{m}(t) = 142.32\ (1 - e^{-0.1246t})$$

and

$$\hat{\lambda}(t) = 17.73 \times e^{-0.1246t}$$

### 4.1.6. Step 6: Application of Predicted Fault Rates

At this stage, the obtained error distribution and the predicted error distribution (based upon the equation used to compute expected number of remaining faults) can be plotted and compared (see figure 4.1-4; Goel, 1983).

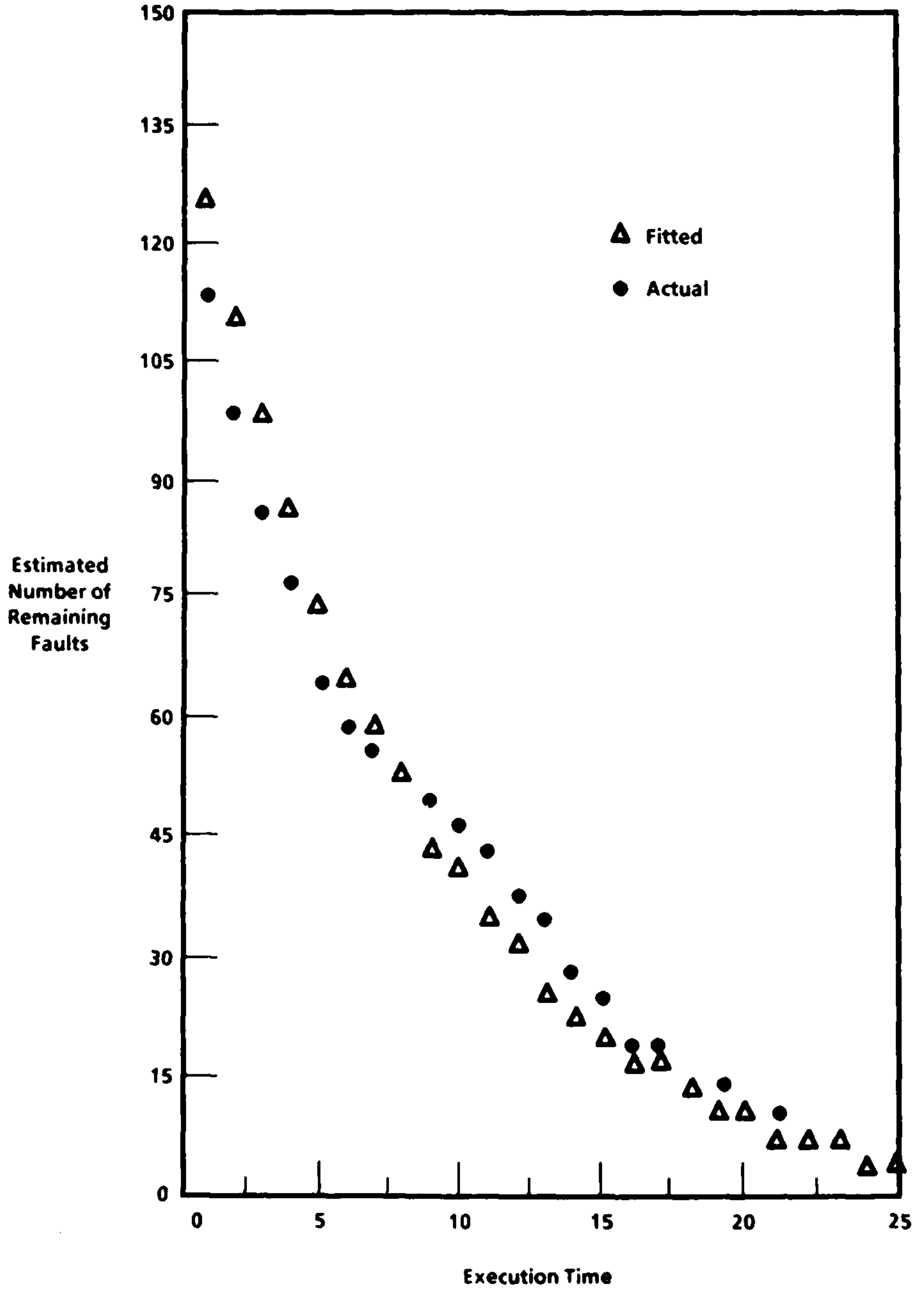


FIGURE 4.1-4. PREDICTED VERSUS ACTUAL NUMBER OF REMAINING FAULTS (from Goel, 1983)

In order to ensure that the predicted model fits the obtained data, goodness-of-fit tests should be applied. If the model fits, results of the reliability modeling process can be appropriately used to make decisions about the software program, for example, to determine whether further testing is required. If the model does not fit, additional testing and data collection may be needed and the process may have to be repeated either using the same model or a more appropriate model based upon the additional data.

## 4.2. Computation of a Time-Between-Failures Model

In section 4.1, the Goel-Okumoto model, a fault-count model which assumes a poisson distribution, was described in some detail. In Steps 1 and 2, if the data generated from the testing had been exponentially distributed and met the assumptions of one of the time-between-failure models, a different model would have been selected, such as the Jelinski-Moranda De-Eutrophication Model. Steps 3 through 5 would then have been performed as follows:

### 4.2.1. Step 3: Model Selection

As before, the assumptions of the selected model must be matched with the characteristics of the data. Assume a set of data which matches the assumptions of the Jelinski-Moranda model (see table 4.2-1; Goel, 1983).

### 4.2.2. Step 4: Statistical Computation to Obtain Parameter Estimates (from Goel, 1983)

The time between the (i-1)st and the ith failures $T_i$, is distributed exponentially with parameter $\Phi[N - (i-1)]$.

$$\text{pdf of } T_i\text{: } f(t_i) = \phi[N - (i-1)]\exp[-\phi\{N - (i-1)\}t_i]$$

$$\text{cdf of } T_i = F(t_i) = 1 - \exp[-\phi\{N-(i-1)t_i\}]$$

A series of n failures is observed with interfailure times as $t_1, t_2, \ldots, t_n$. Usually, the method of maximum likelihood is used to estimate the parameters N and $\Phi$ as shown below.

The likelihood function of N and $\Phi$ is

$$L(N, \phi \mid t_1, t_2, \ldots, t_n) = \prod_{i=1}^{n} \phi[N - (i-1)]\exp[-\phi\{N - (i-1)\}t_i]$$

TABLE 4.2-1. ASSUMPTIONS FOR THE JELINSKI-MORANDA DE-EUTROPHICATION MODEL (from Goel, 1983)

- Initial fault content:

  An unknown fixed constant N.

- Independence of faults:

  Each fault in the program is independent of other faults and each of them is equally likely to cause a failure during testing. Times between occurrences of faults are independent of each other.

- Fault removal process:

  A detected fault is removed with certainty at the end of each testing interval.

  Only one fault is removed during each testing interval.

  The fault removal time is negligible.

  No new faults are introduced during the fault removal process.

- Hazard function:

  The software failure rate of the hazard function during a failure interval is constant and is proportional to the current fault content of the tested program. Thus, during the ith testing interval,

$$z(t_i) = \Phi\{N - (i-1)\},$$

  where $\Phi$ is a proportionality constant, and N is the initial number of faults in the program.

The Maximum Likelihood Estimates (MLE) of N and Φ are obtained by solving the following pair of equations simultaneously.

$$\sum_{i=1}^{n} \frac{1}{N-(i-1)} - \sum_{i=1}^{n} \phi t_i = 0$$

and

$$\frac{n}{\phi} - \sum_{i=1}^{n} [N-(i-1)] t_i = 0$$

The above two equations yield

$$\sum_{i=1}^{n} \frac{1}{N-(i-1)} = \frac{n}{N - \frac{1}{T} \sum_{i=1}^{n} (i-1)t_i} ,$$

where

$$T = \sum_{i=1}^{n} t_i .$$

The above equations can be solved numerically to find $\hat{N}$ and then $\hat{\Phi}$ can be obtained from the following equation.

$$\hat{\phi} = \frac{n}{NT - \sum_{i=1}^{n} (i-1)t_i}$$

Using the asymptotic properties of the maximum likelihood estimators, it can be shown that

$$\mathrm{Var}(\hat{N}) = \frac{n}{\phi 2} \cdot \frac{1}{\det A}$$

$$\mathrm{Var}(\hat{\phi}) = \Sigma \left( \frac{1}{N-i-1} \right)^2 \cdot \frac{1}{\det A}$$

$$\mathrm{Cov}\,(\hat{N},\hat{\phi}) = - \frac{T}{\det A}$$

$$\rho_{\hat{N},\hat{\phi}} = - \frac{T\phi}{\sqrt{n} \cdot \sqrt{\Sigma_2}},$$

where

$$\det A = \frac{n}{\phi 2} \sum_{i=1}^{n} \left( \frac{1}{N-i+1} \right)^2 - T^2,$$

and

$$\Sigma_2 = \sum_{i=1}^{n} \frac{1}{(N-i+1)^2}$$

### 4.2.3. Step 5: Computation of Performance Statistics

Reliability at time t after the nth failure is

$$R_n(t) \equiv P(T_{n+1} > t) = \exp[-\phi\{N-n\}t]$$

MTTF after n failures is

$$\mathrm{MTTF}_n = \int_0^{\infty} R_n(t)dt = \frac{1}{\phi[N-n]}$$

Using the variance-covariance of $\hat{N}$, $\hat{\Phi}$, it can be shown that

$$\text{Variance}\,[R_n(t)] = \frac{e^{-2\Phi_1(N-n)t}}{\det A}\{nt^2 - 2(N-n)Tt^2\phi + (N-n)^2t^2\Sigma_2\}$$

$$\text{Variance}\,(\mathrm{MTTF}_n) = \frac{1}{\det A}\left[\frac{1}{\phi 2}v_1^2 - 2Tv_1v_2 + v_2^2\Sigma_2\right],$$

where

$$v_1 = -\frac{1}{(N-n)^2\phi}$$

$$v_2 = -\frac{1}{(N-n)\phi^2}\text{, and}$$

$\Sigma_2$ and det A are as defined before.

All the above quantities can be computed by replacing N and $\Phi$ by $\hat{N}$ and $\hat{\Phi}$, respectively.

Worked examples of the Goel-Okumoto and Jelinski-Moranda models are provided in appendices C and D.

# 5. FAULT-TOLERANT SOFTWARE

## 5.1. Introduction

Fault-tolerant software is a redundancy technique that is currently being proposed for use in aircraft avionics/electronics applications where system failures are potentially disastrous, and where high reliability is required. The most widely used methods for implementation are the RB and N-version programming, which are roughly analogous to the hardware redundancy techniques of "standby sparing" and multiple modular redundancy. These fault-tolerant features for software are primarily aimed at overcoming the effects of errors in software design and coding; however, they may also compensate for failures due to hardware design deficiencies or malfunctions in input/output channels, depending upon how the versions are implemented. Fault-tolerant software by its very nature tries to incorporate techniques which will ensure that service is maintained by coping with any faults that remain after the application of all fault avoidance measures. In that respect, it does not rely on completion of validation or testing efforts, which can only establish the presence of errors but cannot assure their absence.

## 5.2. Principles of Fault Tolerance

Anderson and Knight (1982) identify four phases into which fault-tolerance techniques can be divided:

"1. ERROR DETECTION. In order to tolerate a fault its effects must first be detected. Clearly, this can only be achieved by performing checks to determine whether any erroneous situation has arisen.

2. DAMAGE ASSESSMENT. Having detected that the system is in error, it will usually be necessary to identify how much of the state of the system has been corrupted.

3. ERROR RECOVERY. Probably the most important aspect of fault tolerance is the provision of an effective means of transforming an erroneous state of the system into a well defined and error free state. Methods for achieving this transformation can sometimes make good use of the information retained in the erroneous state, but it can be more secure to simply discard the erroneous state and reset the system to some prior state (a recovery point).

4. CONTINUED SERVICE. In order to enable the system to continue to provide the service required by its specification, further action may be needed to ensure that the fault whose effects have been obviated does not immediately recur and thus ruin the whole

avionics applications, and the fault/failure data from these efforts are only now becoming available. It is expected that the two fault-tolerant software approaches will be verified and validated using the emerging database.

### 5.4. A Hierarchical Software Reliability Model

This part of the tutorial will describe the hierarchical software reliability model developed by Hitt, E. F., J. J. Webb, and M. S. Bridgeman (Prater, Hitt, and Eldredge, 1986) to predict the reliability of fault-tolerant software prior to its development (i.e., coding). Fault-tolerant software consists of individual software modules, such as single-version software, NVS, decision algorithms, RBs, and acceptance tests. In the model, these modules are treated as separate "function blocks," similar to piece-parts in hardware reliability modeling. Each function block is subject to specific types of faults.

### 5.4.1. Software Components

#### 5.4.1.1. Single Version Software

This is a probabilistic model of deterministic or random events. The program execution is usually deterministic, and the development process is probabilistic. Single version software contains characteristic faults that must be accounted for. Examples of these faults are as follows:

- Incorrect specification.
- Misunderstood or unclear specification.
- Algorithmic error (sometimes called a computational or logic error).
- Input data error.
- Program logic error.
- Output data error.

#### 5.4.1.2. N-version Software

This software is a fault-tolerant software technique which implements two or more functionally equivalent versions, usually in parallel. These versions may be produced independently by separate programming teams, or they may be designed differently by examining and forcing differences into the versions. Upon comparison of the alternate versions, the faults should be distinguishable. Some of the faults associated with NVS include:

- Specification error.
- Performance error (due to incomplete, inconsistent, or ambiguous specifications).

- Non-termination error.

- Algorithmic error.

- Input data error.

- Output data error.

5.4.1.3. Decision.Algorithm

The decision algorithm determines the specific output. This algorithm may be a majority vote, a median select, a bit-by-bit comparison (with the number of bits that are to be compared or that are significant specified), or an average. Considerations to be made in this software design are as follows:

- The type of decision algorithm used.

- The allowable range of discrepancy of each input from all other inputs to the decision algorithm.

- The data sensitivity of the decision algorithm.

5.4.1.4. Recovery Block

The RB method is a fault-tolerant software technique that provides alternate components which may be switched in (usually serially) to replace a faulty component that has been rejected by the acceptance test. These alternate components are designed independently from the main software component (the primary alternate). They generally provide only partial functionality of the software component. The alternate components perform a reduced and simplified function. Prior to entering an alternate, the conditions existing just before entry to the primary alternate are restored. Some examples of faults that occur in the software for RBs include:

- Specification error.

- Performance error.

- Non-termination error.

- Algorithmic error.

- Input data error.

- Output data error.

5.4.1.4.1. Forward Recovery Block

A forward RB restores the system to a consistent state by compensating for inconsistencies found in the current state. For a single process, the forward RB technique requires a complete understanding of the extent of damage and a scheme for correcting the inconsistencies. Exception values (or ranges) must be specified for each data abstraction. These exceptions are specified in response to run-time attempts to violate inherent invariant properties. These anticipated faults can be managed by forward RB techniques.

### 5.4.1.4.2. Backward Recovery Block

Backward RB techniques require the restoration of the system to the last correct state. This is referred to as rollback. The computation resumes from that point. Unanticipated faults, i.e., design faults, are managed by a default exception handler using automatic backward recovery.

### 5.4.1.5. Acceptance Test

An acceptance test checks the acceptability of data generated by a software component. This is usually implemented in software as a logical expression or algorithm. The faults associated with an acceptance test include:

- Specification error.
- Performance error.
- Algorithmic error.
- Input data error.
- Output data error.

### 5.4.1.6. Rollback

The rollback restores the software to the condition existing prior to the execution of an incorrect or faulty version. The rollback resets the software to the original input state allowing the next version to run.

A rollback is used in connection with RB and hybrid NVS systems. Faults that are characteristics of rollback are:

- Specification error.
- Input data error.
- Output data error.
- Unrecoverable state.

### 5.4.1.7. Roll-Forward

The roll-forward is always used in conjunction with a forward RB. The roll-forward transfers the restored state obtained from the forward RB to a forward position in the system. The state for which the forward RB has compensated determines the forward position for this transfer. Faults associated with roll-forward include:

- Specification error.

- Performance error.

- Input data error.

- Output data error.

5.4.2. Inputs to the Software Reliability Model

Software reliability in this model is estimated from the individual probability reliability values (or safety, availability, or accuracy values, if desired) for each function block. Values for each block are either obtained from a software reliability database (which is emerging or assumed to exist), estimated by the lines of code (and the language), derived experimentally by subjecting the function block's software to a number of test cases and counting the failures to determine a reliability value, or obtained from lower (detailed) level models. The reliability values must be real numbers with a range of 0.0 ≤ probabilistic reliability value (or safety, availability, or accuracy value) ≤ 1.0.

5.4.3. Outputs from the Software Reliability Model

The output of the software reliability model is an overall probability reliability value (or safety, availability, or accuracy values, if desired) for the software as a whole. Reliability values can also be estimated for a specific subset of modules within the software.

5.4.4. Model Representation

Control system notation is used to represent the model. Each software module represents a transformation of input to output. Therefore, the reliability value for an individual module estimates the probability of the desired input/output transformation actually occurring. Similarly, input/output transformations taking place through the interaction of multiple modules can also be represented, allowing similar probability estimations of the likelihood that the transformation will occur. Examples of the application of control system notation to reliability estimation are shown in figures 5.4-1 (Prater, Hitt, and Eldredge) through 5.4-6. These figures are explained in more detail below.

5.4.5. The Modeling Process

The Hitt, E. F., J. J. Webb, and M. S. Bridgeman model was developed to allow software reliability estimation prior to actual software development and coding. This model is intended to be used with a computer software applications package designed to allow alternate versions of the same software architecture to be evaluated. Once a preliminary software architecture has been developed and decisions have been made as to anticipated number of N-versions, etc., these decisions can be entered into the computer. Specifically, the software developer can choose the appropriate modules from a menu system such as that shown in table 5.4-1. With the proposed applications software package, the selected set of module types can then be shown on the computer display in the form of a block diagram.

TABLE 5.4-1. RELIABILITY MODEL MENU SELECTIONS
(from Prater, Hitt, and Eldredge, 1986)

- Structure Functional Modules
    - Single version software
    - NVS (The number of versions must be specified by the user.)
    - Decision algorithm
    - Recovery block (The number of alternates must be specified by the user.)
    - Acceptance test
    - Rollback
    - Roll-forward
- Transfer Functional Modules
    - Forward path
    - Positive feedback
    - Negative feedback
    - Positive feed-forward
    - Negative feed-forward

By means of this representation, reliability values for each module can be entered and reliability estimates of the preliminary software system obtained. If the reliability estimate is not sufficiently high, the software architecture can then be modified, for example, by adding additional versions for a given N-version module. In this way, progressive iterations can be evaluated until the desired reliability level is attained.

Note that table 5.4-1 (Prater, Hitt, and Eldredge, 1986) lists the decision algorithm and acceptance test independently of the NVS and RBs. This separation is necessary to allow for flexibility in combining individual modules. For example, the decision algorithm and acceptance test can now be used independently, as well as in conjunction with their respective pairs:

- NVS and decision algorithm, and

- Recovery block and acceptance test.

Keeping the decision algorithm and acceptance test as separate entities requires that each NVS, decision algorithm, RB, and acceptance test module have individual reliability values in order to compute the overall software system reliability. This is intended to improve the accuracy of the transfer functions for this portion of the diagram since it will accommodate variations in the implementation of these concepts.

Unfortunately, a software applications package capable of performing iterative reliability estimations is not yet available, in spite of the potential contributions such a tool could make to the process of ensuring high-quality software. Use of the Hitt, E. F., J. J. Webb, and M. S. Bridgeman model is not contingent upon the availability of such an applications package, however. This same concept of selecting individual modules and estimating the reliability of the software as a whole can be used without a software applications package. The steps involved are described below.

### 5.4.6. Detailed Function Blocks

The Hitt, E. F., J. J. Webb, and M. S. Bridgeman model uses the structure of the software (i.e., the expected reliabilities of the individual modules) to predict overall software reliability. Consequently, the accuracy of these predictions depends upon the extent to which the structure is "filled in." Dissecting the structure into progressively finer modules, and determining reliabilities for these modules, leads to greater predictive accuracy.

Figure 5.4-1 provides an example of a software program which has been decomposed into relatively high-level software modules. This example shows how reliability values are substituted for each function block to permit the determination of the overall system reliability. Because the software structure is represented at a very high level, the reliability values may be less predictive than desired. More precise predictions can be obtained if each of the software design techniques (single version software, N-version software, decision algorithm, RB, and acceptance test) are broken down into more detailed function blocks. (For a more finely structured model, see figure 5.4-6.)

Figure 5.4-2 is an overall representation of the functional constructs associated with each of the function blocks. Errors associated with each of these constructs are shown in tables 5.4-2 and 5.4-3. Each module in figure 5.4-1 has a reliability value associated with it. The occurrence of these errors within a specific software module drops the reliability of that module below 1.0.

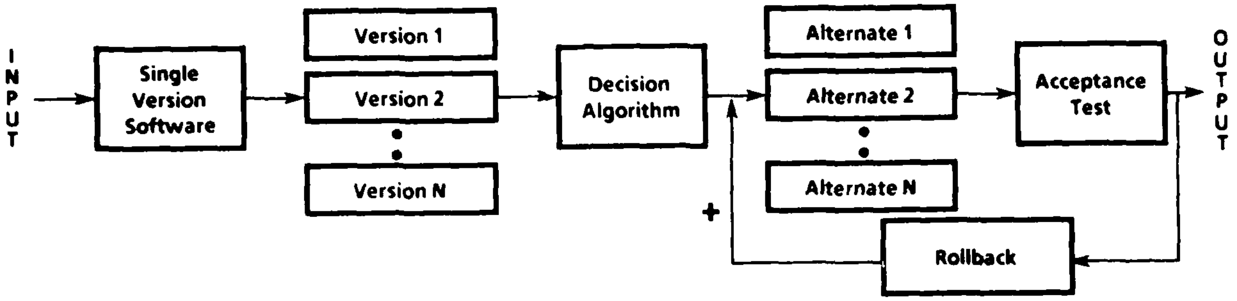


FIGURE 5.4-1. SIMPLE BLOCK DIAGRAM EXAMPLE
(from Prater, Hitt, and Eldredge, 1986)

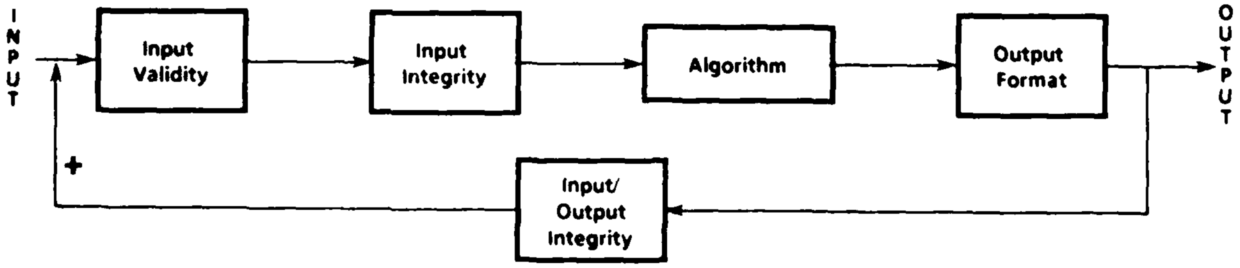


FIGURE 5.4-2. OVERALL REPRESENTATION OF THE FUNCTIONAL CONSTRUCTS
(from Prater, Hitt, and Eldredge, 1986)

TABLE 5.4-2. CORRELATION OF FAULTS WITH THE DETAILED PORTIONS OF THE SINGLE VERSION SOFTWARE FUNCTION BLOCK

| Detailed Function Blocks | | | | | |
|---|---|---|---|---|---|
| Faults | Input Validity | Input Integrity | Algorithm | Output Format | Input/ Output Integrity |
| Incorrect Specification | X | X | X | X | X |
| Misunderstood or Unclear Specification | X | X | X | X | X |
| Algorithmic Error | X | X | X | X | X |
| Input Data Error | X | | | | X |
| Program Logic Error | X | X | X | X | X |
| Output Data Error | | | | X | X |

### 5.4.7. Function Block States

The four possible states for any function block are as follows:

- The function block fails (an error is detected in the function block) and it is corrupt (contains one or more error).
- The function block passes, yet it is corrupt.
- The function block fails and it is error free.
- The function block passes and it is error free.

A mathematical truth table for these states is given in table 5.4-4.

TABLE 5.4-3. CORRELATION OF FAULTS WITH THE DETAILED PORTIONS OF THE DECISION ALGORITHM FUNCTION BLOCK

| | Detailed Function Blocks | | | | |
|---|---|---|---|---|---|
| Faults | Input Validity | Input Integrity | Algorithm | Output Format | Input/ Output Integrity |
| Input Range Error | X | X | | | |
| Algorithmic Error | X | X | X | X | X |

TABLE 5.4-4. TRUTH TABLE OF FUNCTION BLOCK STATES

| State | Error Exists in the Function Block | Error Detected in the Function Block | Error Corrected in the Function Block | Safe | Reliable | Available |
|---|---|---|---|---|---|---|
| a | T | T | T | T | T | T |
| a | T | T | F | T | T* | F |
| b | T | F | N/A | F | F | F* |
| c | F | T | N/A | T | F | F |
| d | F | F | N/A | T | T | T |

<u>Key</u>: N/A - not applicable
* - true or false (the common interpretation is given)

### 5.4.8. System Reliability

The function blocks will each have an associated transfer function ("reliability"). Block diagram reduction techniques can then be used to determine overall system reliability while signal-flow diagram reduction techniques provide the overall system transfer function ("reliability"). The signal-flow diagram is useful in analyzing multiple-loop feedback systems and in determining the effect of a particular element or parameter in an overall feedback system, whereas the block diagram is useful in the design and analysis of sections of a feedback system. Block diagram reduction techniques become tedious and time consuming as the number of feedback paths increases. To solve complex problems, it is much simpler to use the theorems and properties of signal-flow graphs.

### 5.4.9. General Equations

The equations used in this analysis follow S. J. Mason's theorems on the properties of signal-flow graphs. The general expression for the (closed loop) system transfer function using the signal-flow diagram reduction technique is given by

$$\text{Reliability} = \frac{\Sigma_K G_K \Delta_K}{\Delta}$$

where

$$\Delta = 1 - \Sigma L_1 + \Sigma L_2 - \Sigma L_3 + \ldots + (-1)^n \Sigma L_n,$$

$L_1$ = the gain of each closed loop in the graph,

$L_2$ = the product of the loop gains of any two non-touching closed loops,

$L_3$ = the product of the loop gains of any three non-touching closed loops,

$L_n$ = the product of the loop gains of any n non-touching closed loops,

$G_K$ = the gain of the Kth forward path,

$\Delta_K$ = the value of $\Delta$ for that part of the graph not touching the Kth forward path (Shinners, 1978).

The transfer function for NVS and RBs are dependent upon the number of versions or alternates (n).

### 5.4.10. N-version Software Calculations

The transfer function for NVS is given by the following expression:

$$1 - \pi_{i=1}^{C_n} (1 - \alpha_i)$$

with

$n$ = the number of versions in the N-version Software;

$Cn$ = $(n,z)$ = the number of z combinations of the n element set;

$\alpha_i$ = the product of reliabilities of the ith combination required for success; and

$i = 1, 2, \ldots .Cn.$

$z = [(n/2) + 1]$ if n is an even number.

$z = [(n+1)/2]$ if n is an odd number.

The examples in this section and appendix E utilize this equation.

### 5.4.11. Recovery Block Calculations

The transfer function for a RB is dependent upon the number of alternates (n) that are used. This transfer function is calculated with the following equation:

$$G_1 + (1 - G_1)G_2 + (1 - G_1)(1 - G_2)G_3 + \ldots .$$

with $G_i$ = the reliability value for alternate i and

$i = 1, 2, 3, \ldots n.$

The examples in this section and appendix F demonstrate the determination of the overall software reliability value with this equation and the software reliability model.

The reliability values (transfer functions) for the hybrid NVS and the RB will vary if not all of the N versions or N alternates are used. The above equations will give a higher reliability value than the actual situation in these cases. Section 5.4.16 discusses the accuracy of the reliability values for the NVS and RB and how they can be calculated to reflect the actual situation.

Although the transfer function for most of the function blocks is the reliability value, one exception to this is with rollback or any feedback block. For any feedback path, the transfer function of the equivalent block in the path is (1.0 - reliability value). The second exception is with feed-forward paths. The transfer function of the equivalent block in a feed-forward path (for example, roll-forward) is (1.0 - reliability value).

### 5.4.12. Examples of Potential Models: Simple, High-Level Model Example

For a sample problem involving a simple, high level model, the example given in figure 5.4-3 will be used. The single-version software will be a commonly used algorithm or process, and therefore, it will have a high reliability which is well documented and stored in the software reliability database. For this example, the reliability will be 0.9991.

The NVS will have three independent versions, running in parallel. This is a common form of NVS, but not one with the highest reliability. Through the user's tests, it is determined that this function block will have a reliability of 0.994.

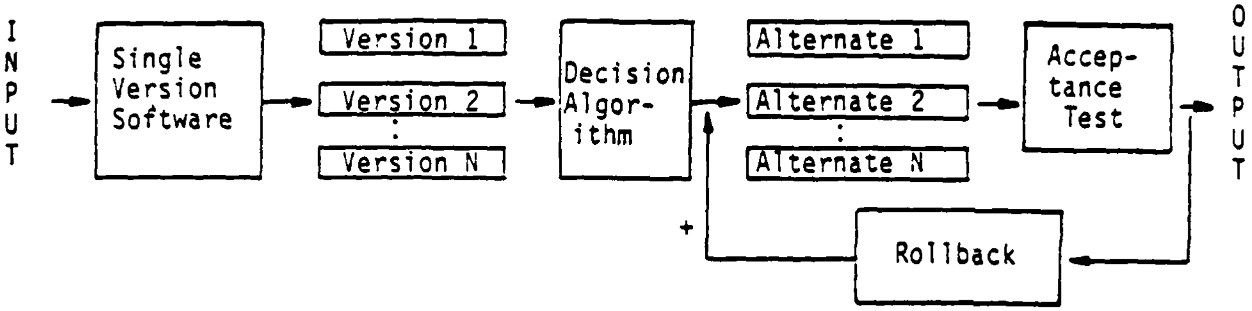


FIGURE 5.4-3. SIMPLE BLOCK DIAGRAM EXAMPLE (from Prater, Hitt, and Eldredge, 1986)

The decision algorithm will take an average of the outputs from the NVS, excluding any version which does not meet the timing constraints. This type of decision algorithm has a high reliability since it does not have a range check or any other source for determining the validity of the output. This decision algorithm will not eliminate any erroneous outputs and will not detect the occurrence of correlated faults. The decision algorithm is simple (and consequently highly reliable), but it is not always the most desirable since its simplicity detracts from its capability of detecting errors. For this example, it is assumed that the reliability of the decision algorithm is 0.988.

The RB is a backward RB with a primary alternate and two additional, extremely simplified alternates. The RB is of a common form and its reliability can be obtained from the software reliability database. For this example, it will have a reliability value of 0.97.

The acceptance test is an output format check. This is a simplistic algorithm that is commonly used in various models. The reliability, as determined from the software reliability database, will be 0.9997.

Finally, the rollback recovers the input state of the software to its condition upon entry to the RB. This is a retrieval of the data from its memory location. The reliability of this common form of Rollback will be assumed to be available in the software reliability database. For this example, the reliability is 0.9999. This makes the transfer function for the rollback equal to (1.0 - 0.9999).

Hence, for this example,

$L_1$ = (0.97) x (0.9997) x (+1.0 - 0.9999) = 0.0000969709

$L_2$ through $L_n$ = 0

$G_1$ = (0.9991) x (0.994) x (0.988) x (0.97) x (0.9997)

= 0.951467

$G_2$ through $G_K$ = 0

$\Delta_1$ = 1

$\Delta$ = 1 - (+0.0000969709) = 0.99990302

Therefore,

$$\text{Reliability} = \frac{(0.951467) \times (1)}{(0.99990302)} = 0.951559$$

Reliability = 0.95

5.4.13. Simple, Detailed Level Model Examples

An example of a simple, detailed level model is given in figure 5.4-4. For this example, the structure functional modules would all be single-version software and the transfer functional modules would be either forward path or positive feedback. Hence, an equivalent block diagram for this detailed block diagram is given in figure 5.4-5.

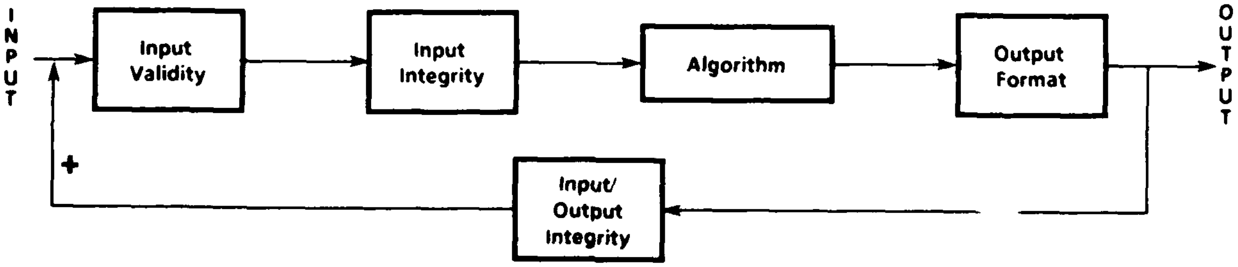


FIGURE 5.4-4. DETAILED DIAGRAM FOR THE SINGLE VERSION SOFTWARE FUNCTION BLOCK OR THE DECISION ALGORITHM FUNCTION BLOCK

In figure 5.4-5, block 1 is a single-version software block which checks the input set. This is a common process, so the reliability value will be assumed to be available in the software reliability database. For this example, the reliability value for block 1 is assumed to be 0.98.

Block 2, a single-version software block, will represent an input integrity check. It will be assumed that this algorithm is common and can consequently be found in the software reliability database. For this example, the reliability value will be 0.97.

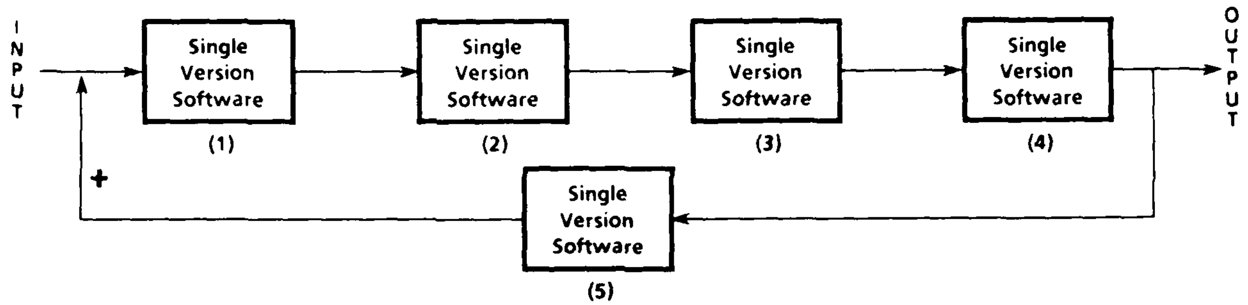


FIGURE 5.4-5. EQUIVALENT DIAGRAM INDICATING THE FUNCTIONAL STRUCTURE TO BE USED IN THE DETAILED DIAGRAM FOR A SINGLE VERSION SOFTWARE FUNCTION BLOCK

Block 3 is a single-version software block which performs an algorithm. For this example, the algorithm will be a simple one. Therefore, the reliability value for this transfer block will be assumed to be 0.992.

Block 4 will represent an output format check, performed by a single-version software block. For this example, the reliability value for this single-version software will be 0.996.

The final single-version software block, block 5, will be used to perform the input/output integrity check in which the output is checked against the input to verify the integrity of the input data. For this example, the reliability value for block 5 will be 0.964. Hence, the transfer function for this block will be (1.0 - 0.964).

Thus, for this example,

$$L_1 = (0.98) \times (0.97) \times (0.992) \times (0.996) \times (1.0 - 0.964)$$

$$= 0.033812$$

$L_2$ through $L_n = 0$

$G_1 = (0.98) \times (0.97) \times (0.992) \times (0.996) = 0.9392232$

$G_2$ through $G_K = 0$

$\Delta_1 = 1$

$$\Delta = 1 - (0.033812)$$

$$= 0.966188$$

Therefore,

$$\text{Reliability} = \frac{(0.9392232) \times (1)}{(0.966188)} = 0.9720916$$

$$\text{Reliability} = 0.97$$

5.4.14. Complex, High-Level Model Example

The complex, high level model example is shown in figure 5.4-6. Block 1 is a single-version software block. For this example, it will be a simple algorithm with a reliability value of 0.998.

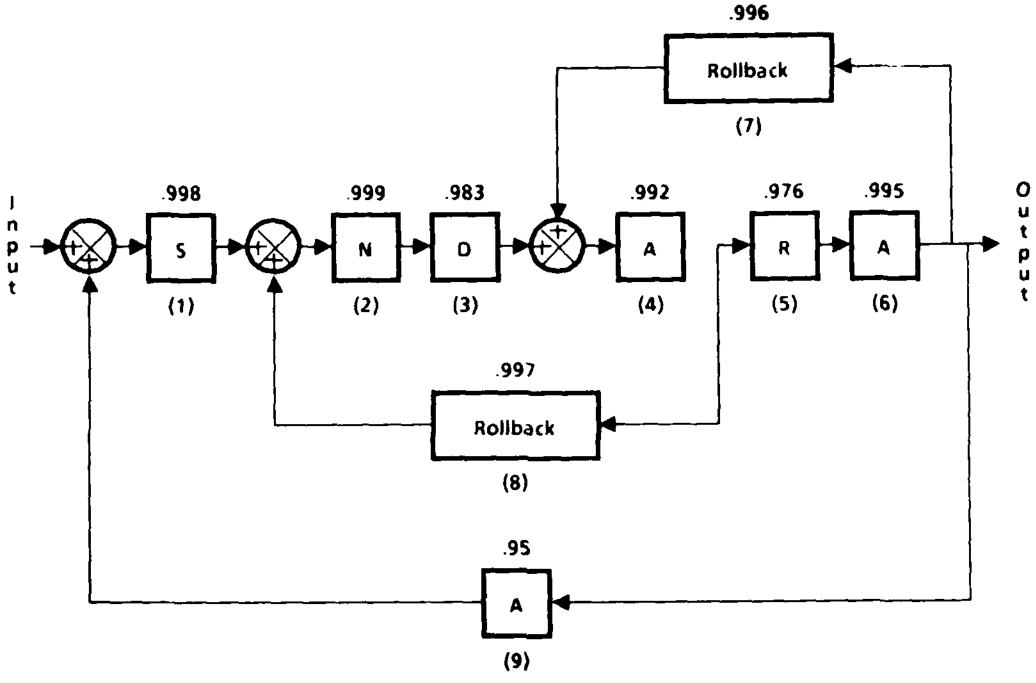
Block 2 is NVS with nine independent versions in which only three versions are run at a time. For this example, it is assumed that the reliability value for the NVS is 0.999.

Block 3 is the decision algorithm for the NVS. In this example, the decision algorithm will be median select with a reliability value of 0.983.

Block 4 is an acceptance test which will check that the range of the output from the decision algorithm is correct. If the decision algorithm failed, then the software will rollback after the acceptance test. Similarly, if the acceptance test fails, then the software will rollback to the NVS. The input to the acceptance test will be stored to accommodate for the rollback from the RB. For this example, the reliability value for the acceptance test will be 0.992.

Block 5 is a RB of the common form with a primary and two additional alternates. For this example, the reliability value of the RB will be 0.976.

Block 6 is the acceptance test for the RB. In this example, it is assumed that the reliability value for this acceptance test is 0.995.



Key:

(1) Single Version Software
(2) N-version Software
(3) Decision Algorithm
(4) Acceptance Test #1
(5) Recovery Block
(6) Acceptance Test #2
(7) Rollback #1--Backward Recovery Block
(8) Rollback #2--N-version Software in Which Only x Versions are Used at a Time
(9) Acceptance Test #3

FIGURE 5.4-6. COMPLEX, HIGH LEVEL MODEL EXAMPLE

The rollback for the backward RB is given in block 7. This is a retrieval of the data that was stored prior to entry into Acceptance Test #1 (Block 4). For this example, the reliability value for this rollback is 0.996. Thus, the transfer function for this block is (1.0 - 0.996).

The rollback for the NVS is given in block 8. For this example, the reliability value is 0.997. Consequently, the transfer function is (1.0 - 0.997).

Finall·, block (9) is an acceptance test which checks the final output against the input. For this example, Acceptance Test #3 will have a reliability value of 0.95, giving a transfer function of (1.0 - 0.95).

Hence, for this example,

$$\text{Closed Loop 1} = (0.999) \times (0.983) \times (0.992) \times (1.0 - 0.997)$$

$$= 0.0029225$$

$$\text{Closed Loop 2} = (0.992) \times (0.976) \times (0.995) \times (1.0 - 0.996)$$

$$= 0.0038534$$

$$\text{Closed Loop 3} = (0.998) \times (0.999) \times (0.983) \times (0.992) \times$$

$$(0.976) \times (0.995) \times (1.0 - 0.95)$$

$$= 0.0472068$$

$$\Sigma L_1 = (\text{Closed Loop 1}) + (\text{Closed Loop 2}) + (\text{Closed Loop 3})$$

$$= 0.0029225 + 0.0038534 + 0.0472068$$

$$= 0.0539827$$

$L_2$ through $L_n = 0$

$$G_1 = (0.998) \times (0.999) \times (0.983) \times (0.992) \times (0.976) \times (0.995)$$

$$= 0.944135$$

$G_2$ through $G_K = 0$

$\Delta_1 = 1$

$$\Delta = 1 - (0.0539827) = 0.9460173$$

Therefore,

$$\text{Reliability} = \frac{(0.944135) \times (1)}{(0.9460173)} = 0.9980103$$

$$\text{Reliability} = 0.998$$

5.4.15. Detailed Worked Examples

Appendices E and F contained detailed worked examples of both N-version and RB systems.

### 5.4.16. Accuracy Constraints

The accuracy and reliability of the NVS, decision algorithm, RB, and acceptance test are dependent upon the way in which these concepts are implemented. For example, NVS may be implemented in one of the following two ways:

- The x of the N-versions are run at a time, and if these versions fail for some reason, then x or fewer of the remaining (n-x) versions are run.

- A combination of x versions is run, and if these x versions fail for some reason, a different combination of x versions is run, and so on.

  NOTE: This concept is different from the first item above, because this implementation groups different combinations of x versions. The first item, however, uses x versions, and if they fail, the x versions are in essence thrown out, and a completely new group of x versions are used; not a new combination of x versions, but x completely new versions.

Some of the differences which affect the reliability and accuracy of the decision algorithm are:

- Majority vote.

- Median select.

- Average.

- The decision algorithm only considers those values which are in certain range and then it uses one of the methods above.

A few of the items which affect the RB's accuracy and reliability are:

- Backward.

  - How far it rolls back.

  - The number of alternates available.

- Forward.

  - How far it rolls forward.

  - The accuracy of the value(s) assigned prior to the roll.

Some of the variables affecting the accuracy and reliability of the acceptance test are:

- The range of the values accepted.

- The rate of change determination for the variables.

- The format of the data.

Needless to say, all of these implementation characteristics must be considered and will affect the accuracy of the reliability values. With this software reliability model design, the accuracy is improved since these considerations can be taken into account in the assignment of reliability values (or accuracy or safety or availability values) to the function blocks.

### 5.4.17. Accuracy

The accuracy of the software reliability model will depend upon the accuracy of the individual values that are used as the transfer functions for each of the function blocks. In most cases, the accuracy of a model with detailed function blocks will be better than the high level software reliability model since the accuracy of the individual transfer functions will be improved.

The accuracy of the reliability values that are used for the function blocks' transfer functions will depend upon the method used to obtain such values. If the values are obtained from the software reliability database, then the accuracy of these values are indicated in the technical reports for the research method that determined the values. If the values are obtained through the use of a different software reliability model, then the accuracy is dependent on the type of model used. Regardless, accuracy values can be obtained for any and all of the transfer functions, and therefore, an accuracy for the overall software reliability values can be calculated.

### 5.4.18. Accuracy of the Hybrid N-version Software

The accuracy of the hybrid NVS reliability value (or safety or availability values) depends upon the number of versions that are actually used. Usually, if the software is run and only y of the N-versions is used, then the reliability value (or safety or availability values) has been overrated by considering the additional (n-y) versions in the calculation of the transfer function for the hybrid NVS. Certainly, if it is known that only y of the N-versions are actually being used, then the calculation of the transfer function for the NVS should only include those y versions.

### 5.4.19. Accuracy of the Recovery Block

The RB, by definition, consists of n alternates. Of these n alternates, only one is run at a time, and only if that alternate fails will the software rollback and run the next alternate. Hence, if less than the n alternates are actually used, the reliability (or safety or availability) of the RB will generally decrease. Furthermore, this decrease in the RB's transfer function (reliability, safety, or availability value) will cause a decrease in the overall software reliability value (or safety or availability value), calculated with the software reliability model.

### 5.4.20. Safety

Safety is concerned with the state in which the function block fails (an error is detected), but the function block is error free. Although a function block is considered to be unsafe when the system is unreliable, safety also covers this extra state. Hence,

safety = [(the probability that an error exists and it is detected) + (the probability that no error exists)]

or

safety = [1 - (the probability that an error exists and it is not detected)]

while

reliability = [(the probability that an error exists and it is detected) + (the probability that no error exists and no error is detected)]

or

reliability = {1 - [(the probability that an error exists, but the error is not detected) + (the probability that no error exists, but an error is detected)]}

Therefore, safety ≥ reliability.

The software reliability model can also be used to determine the safety of the system. Replacing the reliability values with safety values in each function block yields the safety of the overall system.

### 5.4.21. Availability

As with reliability and safety, availability can be determined through the use of the software reliability model. To do so, the availability values should be used for each function block in the determination of the overall transfer function. By using availability values instead of reliability values, the resultant value will be the availability of the overall system.

The availability values are determined as follows:

availability = [The probability that an error exists, it is detected, and it is corrected) + (the probability that no error exists and no error is detected)]

or

availability = {1 - [(the probability that an error exists, it is detected, but it is not corrected) + (the probability that an error exists and no error is detected) + (the probability that no error exists and an error is detected)]}

Therefore, $0 \leq$ availability $\leq 1.0$. By comparison with reliability and safety, availability $\leq$ reliability $\leq$ safety.

### 5.4.22. Response to Undesired Events

The software reliability model described herein assumes independence between the function blocks. This model neglects the existence of:

- Multiple faults which produce dissimilar outputs but are induced by the same input conditions, or

- Related software design faults causing identical incorrect outputs.

The errors that are manifested by these faults are known as coincident errors and cause a degradation in the reliability (or safety or availability). Therefore, to improve the accuracy of the software reliability model, the coincident errors must be considered. This might be done with an analysis similar to that suggested by Eckhardt and Lee (1985). The analysis makes the assumptions that (1) the input series $X_1$, $X_2$, ...., is stationary and independent and (2) the versions of software components are designed independently (Eckhardt & Lee, 1985).

When evaluating the probability of coincident errors, the area of concern is the NVS. This analysis is interested in the probability that z or more of the functions fail at the same time, with $z = (n/2)$ if n is even and $z = [(n + 1)/2]$ if n is odd. The following analysis will give a conservative estimate (maximum possible) of the probability of coincident errors for the NVS. This value might be subtracted from the transfer function of the NVS block to produce a conservative value (minimum) of the reliability (or safety or availability) of the NVS and consequently a conservative estimate (minimum) of the overall software reliability value (or safety or availability value).

The following equation gives the maximum probability of coincident errors (E).

$$E = \binom{n}{z}^{*} (1-G_L)^{z} + \binom{n}{z+1}^{*} (1-G_L)^{z+1} + \binom{n}{z+2}^{*} (1-G_L)^{z+2} + \ldots . + \binom{n}{n}^{*} \binom{n}{1-G_L}^{n}$$

with n = the number of versions in the NVS:

$G_i$ = the reliability (or safety or availability) value for versions i;

i = 1, 2,...n;

$G_L$ = the largest reliability (or safety or availability) value among the group of r versions being evaluated;

z = (n/2) if n is an even number;

z = [(n + 1)/2] if n is an odd number;

$\binom{n}{r}$ = the number of r combinations of an n element set;

$\binom{n}{r}^*$ = the actual r combinations of $(1 - G_i)$ values for the different versions in an n element set of versions.

### 5.4.23. Assumptions

The assumptions that are frequently made with the various software methods are described below, along with the reasons for such assumptions. These assumptions are grouped logically below the corresponding software type to benefit the reader. In the development of this software reliability model, it is assumed that the software of the function blocks will have complete probabilistic independence. However, paragraph 5.4.21 tries to compensate for the deficiencies resulting from this basic assumption.

Single-version Software

- Errors are not always corrected when detected and new errors may be spawned when correcting errors.
- The time to remove a failure is considered to be negligible and is ignored.
- Inputs which exercise the program are randomly selected.
- The failure rate at any time is proportional to the current number of errors remaining in the program (Prater, Hitt and Eldredge, 1986).

N-version Software

- To benefit from increased reliability, N-version assumes that the probability of a common fault among the versions is extremely low.
- When a fault is determined, the damage incurred is limited to the encapsulation of the individual software version and the overall function that the versions are performing.

Decision Algorithm

- For a majority vote, it is assumed that damage will be limited to the versions in the minority when the decision algorithm is invoked.
- It is possible for a majority vote to yield an incorrect result if a majority of the inputs are incorrect.

Recovery Block

- Faults will manifest themselves within a recovery region.

- The alternate versions of software components are independent; correlated faults are either eliminated or reduced to an acceptably low level.

- The n alternate blocks are independent from the acceptance tests (Hitt, Webb, and Bridgeman, 1984).

Acceptance Test

- The acceptance test will recognize the faults.

## 5.5. Scott et al.'s Model

### 5.5.1. Introduction

A second approach to fault-tolerant modeling is that of Scott et al., (1983, 1984, 1987) who developed "data domain" reliability models for the N-version method, RB method, and for an integrated approach called the Consensus RB Method. The models were based on the assumption that "modules with the same functional behavior produce identical correct answers" and that "modules with distinct error behavior produce errors that are distinct from each other as well as distinct from the correct answer." They also assumed that "considerable care would be taken to create the multiple versions using different programmers working independently. The goal of this independent development would be to produce modules with certain independent execution characteristics. For example, it is desirable that the modules have independent error probabilities, that is, the probability that an error is detected in both module A and module B at the same time is the product of the individual module error probabilities. It usually is not desirable, however, that the modules produce distinct correct answers." (Scott et al., 1984, p. 21-1.)

The data domain reliability models for all three fault-tolerant approaches are presented in paragraphs 5.5.3, 5.5.5, and 5.5.7.

### 5.5.2. Recovery Block (from Scott et al., 1984)

In the RB scheme the problem is to detect a software fault in a program, recover the machine state at the time the faulty program was entered, and execute another program that performs the same function as the faulty one. A number of independently designed programs that perform the same function must be developed. The versions are ranked. When the given task is requested, only the "best" program is executed. If a fault is detected in this program, then the "next best" one is executed, etc., until an acceptable output is obtained. If all versions are deemed faulty, an error is posted.

### 5.5.3. The Recovery Block Reliability Model

In the RB Reliability Model there are four distinct types of errors that can occur in a RB system. A Type 1 error occurs when any program version produces an incorrect result, but the acceptance test labels the result as correct. In a Type 2 error, the final version produces correct results, but the acceptance test erroneously determines that the results are incorrect. A Type 3 error occurs when the recovery program cannot successfully recover the input state of the previous version in preparation for executing another version. Finally, a Type 4 error occurs when the last version produces incorrect results and the acceptance test judges that the results are incorrect.

These error types are roughly equivalent to the function block states identified by Hitt, E. F., J. J. Webb, and M. S. Bridgeman in the previous section of this report. A Type 1 error [$P(A_I)$ below] is equivalent to E1, a Type 2 error [$P(R_I)$ below] to E2, a Type 3 error [$P(R_C)$ below] to E3, and a Type 4 error [$P(A_C)$ below] to E4.

The reliability model presented is developed using the probabilities of certain RB events. These events and their probabilities are:

$P(C_i)$ = PROBABILITY OF VERSION i EXECUTING CORRECTLY

$P(I_i)$ = $1 - P(C_i)$

$P(C_R)$ = PROBABILITY OF THE RECOVERY PROGRAM EXECUTING CORRECTLY

$P(I_R)$ = $1 - P(C_R)$

$P(A_I)$ = PROBABILITY OF ACCEPTING AN INCORRECT RESULT

$P(R_I)$ = PROBABILITY OF REJECTING AN INCORRECT RESULT

= $1 - P(A_I)$

$P(R_c)$ = PROBABILITY OF REJECTING A CORRECT RESULT

$P(A_c)$ = PROBABILITY OF ACCEPTING A CORRECT RESULT

= $1 - P(R_c)$

$P(A_B)$ = PROBABILITY OF THE JOINT EVENT A AND B

$P_{RB}(E_K,N)$ = PROBABILITY OF A TYPE K ERROR GIVEN N-VERSIONS

The probability of each of the four types of errors in a 3-version RB with perfect recovery can be found. Assuming version and acceptance test independence, the probabilities are:

$$\begin{aligned} P_{RB}(E_1,3) = {} & P(I_1)P(A_I) \\ & + P(C_1)P(R_C)P(I_2)P(A_I) + P(I_1)P(R_I)P(I_2)P(A_I) \\ & + P(C_1)P(R_C)P(C_2)P(R_C)P(I_3)P(A_I) \\ & + P(C_1)P(R_C)P(I_2)P(R_I)P(I_3)P(A_I) \\ & + P(I_1)P(R_I)P(C_2)P(R_C)P(I_3)P(A_I) \\ & + P(I_1)P(R_I)P(I_2)P(R_I)P(I_3)P(A_I) \end{aligned}$$

$$\begin{aligned} P_{RB}(E_2,3) = {} & P(C_1)P(R_C)P(C_2)P(R_C)P(C_3)P(R_C) \\ & + P(I_1)P(R_I)P(C_2)P(R_C)P(C_3)P(R_C) \\ & + P(C_1)P(R_C)P(I_2)P(R_I)P(C_3)P(R_C) \\ & + P(I_1)P(R_I)P(I_2)P(R_I)P(C_3)P(R_C) \end{aligned}$$

$$P_{RB}(E_3,3) = 0$$

$$\begin{aligned} P_{RP}(E_4,3) = {} & P(C_1)P(R_C)P(C_2)P(R_C)P(I_3)P(R_I) \\ & + P(I_1)P(R_I)P(C_2)P(R_C)P(I_3)P(R_I) \\ & + P(C_1)P(R_C)P(I_2)P(R_I)P(I_3)P(R_I) \\ & + P(I_1)P(R_I)P(I_2)P(R_I)P(I_3)P(R_I) \end{aligned}$$

If there is dependence among the three program versions, but no dependence between the versions and the acceptance test, the RB model becomes:

$$\begin{aligned} P_{RB}(E_1,3) = {} & P(I_1)P(A_I) + P(C_1I_2)P(R_C)P(A_I) + P(I_1I_2)P(R_I)P(A_I) \\ & + P(C_1C_2C_3)P(R_C)^2P(A_I) + P(C_1I_2I_3)P(R_C)P(R_I)P(A_I) \\ & + P(I_1C_2I_3)P(R_I)P(R_C)P(A_I) + P(I_1I_2I_3)P(R_I)^2P(A_I) \end{aligned}$$

$$\begin{aligned} P_{RB}(E_2,3) = {} & P(C_1C_2C_3)P(R_C)^3 + P(C_1I_2C_3)P(R_C)^2P(R_I) \\ & + P(I_1C_2C_3)P(R_C)^2P(R_I) + P(I_1I_2C_3)P(R_I)^2P(R_C) \end{aligned}$$

$$P_{RB}(E_3,3) = 0$$

$$\begin{aligned} P_{RB}(E_4,3) = {} & P(I_1I_2I_3)P(R_I)^3 + P(I_1C_2I_3)P(R_I)^2P(R_C) \\ & + P(C_1I_2I_3)P(R_I)^2P(R_C) + P(C_1C_2I_3)P(R_C)^2P(R_I) \end{aligned}$$

The probability of getting any error is:

$$P_{RB}(E,3) = P_{RB}(E_1,3) + P_{RB}(E_2,3) + P_{RB}(E_3,3) + P_{RB}(E_4,3)$$

And of course, system reliability is:

$$P_{RB} = 1 - P_{RB}(E,n)$$

### 5.5.4. N-version Programming

Another prevalent method of software fault-tolerance is the N-version Programming method. In this method, n programmers (n > 1) are asked to independently develop and debug a program, each working from a common specification. The n programs are placed under the control of a supervisor program that dispatches all versions of the program with the necessary input when the specified task is required. Upon completion, the outputs of the n programs are compared. Since all versions of the program are independently developed, it is assumed that the probability of a common software error is zero. Therefore, if at least two program versions agree on an output, that output is assumed to be "correct."

### 5.5.5. The N-version Programming Reliability Model

In the N-version Programming Reliability Model, there are three types of errors that can occur in an N-version Programming system. A Type 1 error occurs when all outputs disagree. A Type 2 error occurs when a particular incorrect output occurs more than once. Finally, a Type 3 error occurs when there is an error in the voting procedure. The probability of a system error is then the sum of the three probabilities of a Type 1, 2, or 3 error.

The probability of a Type 1 error in a 2 of 3 N-version Programming system composed of independent program versions is:

$$\begin{aligned} P_{NVP}(E_1,3) &= P(I_1)P(I_2)P(I_3) + P(C_1)P(I_2)P(I_3) + P(I_1)P(C_2)P(I_3) \\ &\quad + P(I_1)P(I_2)P(C_3) \\ &= P(I_1)P(I_2) + P(I_1)P(I_3) + P(I_2)P(I_3) - 2P(I_1)P(I_2)P(I_3) \end{aligned}$$

If the program versions are not independent, then probability of a Type 1 error becomes:

$$\begin{aligned} P_{NVP}(E_1,3) &= P(I_1I_2I_3)P(I_2I_3)P(I_2I_3)P(I_3) + P(C_1I_2I_3)P(I_2I_3)P(I_3) \\ &\quad + P(I_1C_2I_3)P(C_2I_3)P(I_3) + P(I_1I_2C_3)P(I_2C_3)P(C_3) \\ &= P(I_1I_2I_3)P(I_2I_3)P(I_3) + [1 - P(I_1I_2I_3)]P(I_2I_3)P(I_3) \\ &\quad + P(I_1C_2I_3)[1 - P(I_2I_3)]P(I_3) + P(I_1I_2C_3)P(I_2C_3)[1 - P(I_3)] \end{aligned}$$

If the versions are dependent, the probability of a Type 2 error, the multiple occurrence of an incorrect answer, cannot be assumed to be zero. It is still reasonable that a Type 3 error is zero. Therefore, the probability of an error in a dependent N-version Programming system is:

$$P_{NVP}(E,n) = P_{NVP}(E_1,n) + P_{NVP}(E_2,n)$$

Therefore, the reliability of a 2 of 3 N-version Programming system is:

$$R_{NVP} = 1 - P_{NVP}(E,3)$$

### 5.5.6. Consensus Recovery Block (from Scott et al., 1984)

The Consensus RB is a software fault-tolerant technique that combines aspects of RBs and N-version Programming. This hybrid technique attempts to overcome some serious problems in the two established fault-tolerant techniques.

The Consensus RB requires the development of n independent versions of a program, an acceptance test, and a voting procedure. The versions are ranked as in a conventional RB system. Upon invocation of the Consensus RB, all versions execute and submit their outputs to a voting procedure. Since the voting procedure assumed that there are no common faults, if two or more of the versions agree on one output, that output is designated as correct. If there is no agreement, that is, the versions supply incorrect outputs or multiple correct outputs, then a modified RB is entered. The output of the "best" version is examined by the acceptance test. If that output is judged acceptable, it is treated as a correct output and system execution continues. If, on the other hand, the output is not accepted, the next best version's output is subjected to the acceptance test. This process continues until an acceptable output is found, or the n outputs are exhausted. Notice that there is no requirement for input state recovery since all versions execute in a parallel fashion as in an N-version Programming system, not in a serial fashion as in a conventional RB.

### 5.5.7. The Consensus Recovery Block Reliability Model (from Scott et al., 1984)

The probabilities of error in the Consensus RB Reliability Model are the same as those in the RB model multiplied by P(D), the probability of output disagreement. In addition, a new error, Type 5 Error, can occur if there is agreement on an incorrect output. The Type 5 Error in a Consensus RB is analogous to a Type 2 error in an N-version Programming system. Therefore, in a 3-version independent Consensus RB, the probabilities of error are:

$$\begin{aligned} P_{CRB}(E_1,3) = {} & P(D)[P(I_1)P(A_1) + P(C_1)P(R_C)P(I_2)P(A_1) \\ & + P(I_1)P(R_I)P(I_2)P(A_I) + P(C_1)P(R_C)P(C_2)P(R_C)P(I_3)P(A_I) \\ & + P(C_1)P(R_C)P(I_2)P(R_I)P(I_3)P(A_I) \\ & + P(I_1)P(R_I)P(C_2)P(R_C)P(I_3)P(A_I) \\ & + P(I_1)P(R_I)P(I_2)P(R_I)P(I_3)P(A_I)] \end{aligned}$$

$$\begin{aligned} P_{CRB}(E_2,3) = {} & P(D)\ [P(C_1)P(R_C)P(C_2)P(R_C)P(C_3)P(R_C) \\ & + P(I_1)P(R_I)P(C_2)P(R_C)P(C_3)P(R_C) \\ & + P(C_1)P(R_C)P(I_2)P(R_I)P(C_3)P(R_C) \\ & + P(I_1)P(R_I)P(I_2)P(R_I)P(C_3)P(R_C)] \end{aligned}$$

$$P_{CRB}(E_3,3) = 0$$

$$\begin{aligned} P_{CRB}(E_4,3) = {} & P(D)\ [P(C_1)P(R_C)P(C_2)P(R_C)P(I_3)P(R_I) \\ & + P(I_1)P(R_I)P(C_2)P(R_C)P(I_3)P(R_I) \\ & + P(C_1)P(R_C)P(I_2)P(R_I)P(I_3)P(R_I) \\ & + P(I_1)P(R_I)P(I_2)P(R_I)P(I_2)P(R_I)P(I_3)P(R_I)] \end{aligned}$$

$$P_{CRB}(E_5,3) = P(\text{AGREEMENT ON INCORRECT OUTPUT})$$

If there is dependence among the three program versions, but no dependence between the versions and the acceptance test, the Consensus RB model becomes:

$$\begin{aligned} P_{CRB}(E_1,3) = {} & P(DI_1)P(A_I) + P(DC_1I_2)P(R_C)P(A_I) + P(DI_1I_2)P(R_I)P(A_I) \\ & + P(DC_1C_2C_3)P(R_C)^2P(A_I) + P(DC_1I_2I_3)P(R_C)P(R_I)P(A_I) \\ & + P(DI_1C_2I_3)P(R_I)P(R_C)P(A_I) + P(DI_1I_2I_3)P(R_I)^2P(A_I) \end{aligned}$$

$$\begin{aligned} P_{CRB}(E_2,3) = {} & P(DC_1C_2C_3)P(R_C)^3 + P(DC_1I_2C_3)P(R_C)^2P(R_I) \\ & + P(DI_1C_2C_3)P(R_C)^2P(R_I) + P(DI_1I_2C_3)P(R_I)^2P(R_C) \end{aligned}$$

$$P_{CRB}(E_3,3) = 0$$

$$P_{CRB}(E_4,3) = P(DI_1I_2I_3)P(R_I)^3 + P(DI_1C_2I_3)P(R_I)^2P(R_C) + P(DC_1I_2I_3)P(R_I)^2P(R_C) + P(DC_1C_2I_3)P(R_C)^2P(R_I)$$

The probability of getting any error is:

$$P_{CRB}(E,3) = P_{CRB}(E_1,3) + P_{CRB}(E_2,3) + P_{CRB}(E_3,3) + P_{CRB}(E_4,3) + P_{CRB}(E_5,3)$$

And of course, system reliability is:

$$R_{CRB} = 1 - P_{CRB}(E,n)$$

### 5.5.8. Verification

Scott et al., 1984 and 1987, have presented data from a number of experiments conducted in a university environment. The purpose of these experiments was to validate the ability of the three proposed fault-tolerant models to accurately predict system reliability. The data from these experiments, appear to indicate that the RB method and the Consensus RB method can provide the required system reliability, and that the equations developed to represent each of the models can provide the reliability estimates, which in turn can accurately predict system reliability.

## APPENDIX A - ASSUMPTIONS UNIQUE TO FAULT COUNT SOFTWARE RELIABILITY MODELS

This appendix provides a list of the underlying assumptions that are unique to each of the Fault Count Software Reliability Models referenced in section 4 of this report.

- ASSUMPTIONS UNDERLYING THE GOEL-OKUMOTO NON-HOMOGENEOUS POISSON PROCESS MODEL
    - Expected number of software faults to be eventually detected is an unknown fixed quantity.
    - Actual number of faults to be observed is a random variable.
    - Each failure is caused by one fault, and each fault is equally likely to cause a failure during testing.
    - Number of software faults detected during each non-overlapping testing interval is independent of each other.
    - Expected number of software faults detected during $(t, t + \Delta t)$ is proportional to the expected number of software faults undetected by time t.
    - Fault removal time is negligible.
    - No new faults are introduced during the fault removal process.

- ASSUMPTIONS UNDERLYING THE GEOMETRIC POISSON MODEL
    - There is an infinite number of total errors.
    - Each fault in the program is independent of the others and each of them is equally likely to occur.
    - The errors do not have the same likelihood of detection.
    - Data are available only at discrete intervals.
    - During a fixed interval of time, the number of errors detected follows a Poisson distribution.
    - During each of these periods of time, the detection rate is constant.

- Each error discovered is immediately removed or no longer counted.
- No new fault is introduced during the correction process.

- ASSUMPTIONS UNDERLYING THE EXTENDED JELINSKI-MORANDA MODEL

  - There is a fixed number of errors in the program.
  - Each error has an equal chance of being detected.
  - The number of machire language instructions remains relatively constant.
  - The failure rate is proportional to the current error content (number of remaining errors).
  - There is a constant failure rate between consecutive errors.
  - More than one error may occur in a given debugging time period.
  - The program is not being altered except for error correction.
  - No new errors are added during the debugging process.
  - Each error has an equal chance of being detected.

- ASSUMPTIONS UNDERLYING THE MODIFIED GEOMETRIC DE-EUTROPHICATION MODEL

  - The program contains an unknown number of errors.
  - Each fault in the program is independent, and each fault is equally likely to cause a failure during testing.
  - The number of faults detected in any time interval is independent of the number of faults detected in any other time interval.
  - The program is not being altered except for error correction.
  - The error correction time is negligible. Each error discovered is immediately removed.
  - No new errors are added during the debugging process.

- ASSUMPTIONS UNDERLYING THE SHOOMAN EXPONENTIAL MODEL

  - The initial number of errors in a program is a constant.
  - The number of errors remaining in the program decreases as errors are corrected.
  - Each error has an equal chance of being detected.
  - Software errors occur with a probability distribution of

    $$f(t) = \lambda \exp(- \lambda t)$$

  - The error detection rate (failure rate) is proportional to the number of remaining errors.
  - The total number of machine language instructions remains constant.
  - Operational software errors occur due to the occasional traversing of a portion of the program in which a software bug is hidden.

## APPENDIX B - ASSUMPTIONS UNIQUE TO TIME-BETWEEN-FAILURE SOFTWARE RELIABILITY MODELS

This appendix provides a list of the underlying assumptions that are unique to each of the Time-Between-Failure Software Reliability Models referenced in section 4 of this report.

- ASSUMPTIONS UNDERLYING THE JELINSKI AND MORANDA DE-EUTROPHICATION MODEL

  - Initial fault content is an unknown fixed constant n.

  - Each fault in the program is independent of other faults, and each fault is equally likely to cause a failure during testing.

  - Times between occurrences of faults are independent of each other.

  - The software failure rate of the hazard function during a failure interval is constant and is proportional to the current fault content of the tested program.

  - A detected fault is removed with certainty at the end of each testing interval.

  - Only one fault is removed during each testing interval.

  - The fault removal time is negligible.

  - No new faults are introduced during the fault removal process.

- ASSUMPTIONS UNDERLYING THE GEOMETRIC DE-EUTROPHICATION MODEL

  - There is an infinite number of total errors.

  - Each fault in the program is independent of the others and each of them is equally likely to occur.

  - The errors do not have the same likelihood of detection.

  - The failure rate between successive errors forms a geometric progression and is constant in the interval between errors.

  - Each error discovered is immediately removed. The time to correct the detected faults is negligible.

- No new fault is introduced during the correction time.

- ASSUMPTIONS UNDERLYING THE GENERALIZED IMPERFECT DEBUGGING MODEL

  - All failures are observable and independent.
  - Testing is of uniform intensity and representative of the operational environment.
  - Inputs which exercise the program are randomly selected.
  - The failure rate at any time is proportional to the current number of errors remaining in the program.
  - The failure rate between the (i-1)th failure and the ith failure is $\lambda(t_i) = \phi[N-(i-1)]t^{\alpha-1}$.
  - The time to remove a failure is considered to be negligible and is ignored in the model.
  - Errors are not always corrected when detected, and errors may be spawned when correcting errors.

- ASSUMPTIONS UNDERLYING THE BUG-PROPORTIONAL MODEL

  - The initial number of errors in a program is a constant.
  - The number of errors remaining in the program decreases as errors are corrected.
  - Software errors are caused by the uncovering of residual bugs in a program.
  - The probability that a bug is encountered in the time interval, $\Delta t$, after t successful hours of operation is proportional to the fractional number of remaining bugs.
  - The fractional number of remaining bugs is independent of the operating time.
  - The rate of error correction is constant.

## APPENDIX C - WORKED EXAMPLE FOR THE GOEL-OKUMOTO ON-HOMOGENEOUS POISSON PROCESS MODEL

Worked example showing computations for the Goel-Okumoto NHPP Model (Fault Count). This example has been adapted from Goel (1983).

Consider the following failure counts.

| Interval No. | Cumulative No. of Failures |
|---|---|
| 1 | 2 |
| 2 | 4 |
| 3 | 5 |

The parameters to be estimated are a and b, where a is the expected number of software faults to be eventually detected; and b is a proportionality constant.

The MLE of a and b can be obtained by solving the following pair of equations.

$$a(1-e^{-bt_n}) = y_n$$

$$at_n e^{-bt_n} = \sum_{i=1}^{n} \frac{(y_i - y_{i-1})(t_i e^{-bt_i} - t_{i-1} e^{-bt_{i-1}})}{e^{-bt_{i-1}} - e^{-bt_i}},$$

These equations yield

$$\frac{y_n t_n e^{-bt_n}}{(1-e^{-bt_n})} = \sum_{i=1}^{n} \frac{(y_i - y_{i-1})(t_i e^{-bt_i} - t_{i-1} e^{-bt_{i-1}})}{e^{-bt_{i-1}} - e^{-bt_i}}$$

which can be used to obtain the MLE of b by the Newton-Raphson method.

Using the Newton-Raphson method to find $\hat{b}$:

$$\text{Let } F = \sum_{i=1}^{n} \frac{(y_i - y_{i-1})(t_i e^{-bt_i} - t_{i-1} e^{-bt_{i-1}})}{e^{-bt_{i-1}} - e^{-bt_i}} - \frac{y_n t_n e^{-bt_n}}{(1 - e^{-bt_n})}$$

then

$$\frac{dF}{db} = \sum_{i=1}^{n} (y_i - y_{i-1}) \left[ \frac{(e^{-bt_{i-1}} - e^{-bt_i})(t_{i-1}^2 e^{-bt_{i-1}} - t_i^2 e^{-bt_i})}{(e^{-bt_{i-1}} - e^{-bt_i})^2} - \frac{(t_i e^{-bt_i} - t_{i-1} e^{-bt_{i-1}})^2}{(e^{-bt_{i-1}} - e^{-bt_i})^2} \right] + \frac{y_n t_n^2 e^{-bt_n}}{(1 - e^{-bt_n})^2}$$

We can then compute the MLE of a as

$$a = \frac{y_n}{(1 - e^{-bt_n})}$$

For the above data set

$$n = 3,\ t_0 = 0,\ t_1 = 1,\ t_2 = 2,\ t_3 = 3$$

$$y_0 = 0,\ y_1 = 2,\ y_2 = 4,\ y_3 = 5$$

The computation of MLE to Estimate a and b is as follows:

<u>Iteration 1.</u> Let an initial value of b = .01; i.e., $b^{(1)} = 0.01$

Then

$$F = \sum_{i=1}^{3} \frac{(y_i - y_{i-1})(t_i e^{-.01t_i} - t_{i-1} e^{-.01t_{i-1}})}{e^{-.01t_{i-1}} - e^{-.01t_i}} - \frac{y_3 t_3 e^{-.01t_3}}{(1 - e^{-.01t_3})}$$

$$= \frac{y_1 (t_1 e^{-.01t_1})}{1 - e^{-.01t_1}} + \frac{(y_2 - y_1)(t_2 e^{-.01t_2} - t_1 e^{-.01t_1})}{e^{-.01t_1} - e^{-.01t_2}}$$

$$+ \frac{(y_3 - y_2)(t_3 e^{-.01t_3} - t_2 e^{-.01t_2})}{e^{-.01t_2} - e^{-.01t_3}} - \frac{y_3 t_3 e^{-.01t_3}}{(1 - e^{-.01t_3})}$$

$$= \frac{2(e^{-.01})}{1 - e^{-.01}} + \frac{(4 - 2)(2e^{-.02} - e^{-.01})}{e^{-.01} - e^{-.02}} + \frac{(5 - 4)(3e^{-.03} - 2e^{-.02})}{e^{-.02} - e^{-.03}}$$

$$- \frac{5 \cdot 3 \cdot e^{-.03}}{(1 - e^{-.03})}$$

$$= 493.5041667 - 492.5374994$$

$$= .966667222210$$

Now,

$$\frac{dF}{db} = \sum_{i=1}^{3} (y_i - y_{i-1}) \left[ \frac{(e^{-.01t_{i-1}} - e^{-.01t_i})(t_{i-1}^2 e^{-.01t_{i-1}} - t_i^2 e^{-.01t_i})}{(e^{-.01t_{i-1}} - e^{-.01t_i})^2} \right.$$

$$\left. - \frac{(t_i e^{-.01t_i} - t_{i-1} e^{-.01t_{i-1}})^2}{(e^{-.01t_{i-1}} - e^{-.01t_i})^2} \right] + \frac{y_3 t_3^2 e^{-.01t_3}}{(1 - e^{-.01t_3})^2}$$

$$= \frac{y_1[(e^{-0.1x0} - e^{-.01})(-e^{-.01}) - e^{-.01x2}]}{(e^{-.01x0} - e^{-.01})^2}$$

$$+ \frac{(y_3 - y_2)[(e^{-.02} - e^{.03})(4e^{-.02} - 9e^{-.03}) - (3e^{-.03} - 2e^{-.02})^2]}{(e^{-.02} - e^{-.03})^2}$$

$$+ \frac{5 \cdot 9 \cdot e^{-.03}}{(1 - e^{-.03})^2}$$

$$+ \frac{(y_2 - y_1)[(e^{-.01} - e^{-.02})(e^{-.01} - 4e^{-.02}) - (2e^{-.02} - e^{-.01})^2]}{(e^{-.01} - e^{-.02})^2}$$

$$= \frac{2[(1 - e^{-.01})(-e^{-.01}) - e^{-.02}]}{(1 - e^{-.01})^2}$$

$$+ \frac{2[(e^{-.01} - e^{-.02})(-e^{-.01} - 4e^{-.02}) - (2e^{-.02} - e^{-.01})^2]}{(e^{-.01} - e^{-.02})^2}$$

$$+ \frac{1[(e^{-.02} - e^{-.03})(4e^{-.02} - 9e^{-.03}) - (3e^{-.03} - 2e^{-.02})^2]}{(e^{-.02} - e^{-.03})^2}$$

$$+ \frac{45 \cdot e^{-.03}}{(1 - e^{-.03})^2}$$

$$= -\left( \frac{2e^{-.01}}{(1 - e^{-.03})^2} + \frac{2e^{-.03}}{(e^{-.01} - e^{-.02})^2} + \frac{e^{-.05}}{(e^{-.02} - e^{-.03})^2} \right) + \frac{45e^{-.03}}{(1 - e^{-.03})^2}$$

$$= -49999.58334 + 49996.25017$$

$$= -3.33316667270$$

and

$$\Delta b^{(1)} = -F \div dF/db = -.966667222210 \div -3.33316667270$$
$$= .2900146669 > .0001$$

Let $\epsilon$ = 0.0001. Since $\Delta b^{(1)} > \epsilon$, we go to iteration 2.

Iteration 2.

$$b^{(2)} = b^{(1)} + \Delta b^{(1)} = .3000146669 \simeq .3$$

$$F = \sum_{i=1}^{3} \frac{(y_i - y_{i-1})(t_i e^{-.3t_i} - t_{i-1} e^{-.3t_{i-1}})}{e^{-.3t_{i-1}} e^{-.3t_i}} - \frac{y_3 t_3 e^{-.3t_3}}{(1 - e^{-.3t_3})}$$

$$= \frac{2(e^{-.3})}{1 - e^{-.3}} + \frac{2(2e^{-.6} - e^{-.3})}{e^{-.3} - e^{-.6}} + \frac{1(3e^{-.9} - 2e^{-.6})}{(e^{-.6} - e^{-.9})} - \frac{5 \cdot 3e^{-.9}}{(1 - e^{-.9})}$$

$$= 10.2906087 - 10.27600431$$
$$= .0146665525129$$

Now,

$$\frac{dF}{db} = \sum_{i=1}^{3} (y_i - y_{i-1}) \left[ \frac{(e^{-.3t_{i-1}} - e^{-.3t_i})(t_{i-1}^2 e^{-.3t_{i-1}} - t_i^2 e^{-.3_i})}{(e^{-.3t_{i-1}} - e^{-.3t_i})^2} \right.$$
$$\left. - \frac{(t_i e^{-.3t_i} - t_{i-1} e^{-.3t_{i-1}})^2}{(e^{-.3t_{i-1}} - e^{-.3t_i})^2} \right] + \frac{y_3 t_3^2 e^{-.3t_3}}{(1 - e^{-.3t_3})^2}$$

$$= \frac{2[(1 - e^{-.3})(-e^{-.3}) - e^{-.6}]}{(1 - e^{-.3})^2}$$

$$+ \frac{2[(e^{-.3} - e^{-.6})(e^{-.3} - 4e^{-.6}) - (2e^{-.6} - e^{-.3})^2}{(e^{-.3} - e^{-.6})^2}$$

$$+ \frac{1[(e^{-.6} - e^{-.9})(4e^{-.6} - 9e^{-.9}) - (3e^{-.9} - 2e^{-.6})^2]}{(e^{-.6} - e^{-.9})^2} + \frac{45e^{-.9}}{(1 - e^{-.9})^2}$$

$$= -\left( \frac{2e^{-.3}}{(1 - e^{-.3})^2} + \frac{2e^{-.9}}{(e^{-.3} - e^{-.6})^2} + \frac{e^{-1.5}}{(e^{-.6} - e^{.9})^2} \right) + \frac{45e^{-.9}}{(1 - e^{-.9})^2}$$

$$= -55.13532562 + 51.94726586 = -3.18805975584$$

$$\Delta b^{(2)} = -F \div dF/db = -.0146665525129 \div -3.18805975584$$
$$= .004600463491$$

Since $\Delta b^{(2)} > \epsilon$, we continue the computations.

Iteration 3.

$$b^{(3)} = b^{(2)} + \Delta b^{(2)} = .3000146669 + .004600463491$$
$$= .30461513036 \approx .305$$

$$F = \sum_{i=1}^{3} \frac{(y_i - y_{i-1})(t_i e^{-.305t_i} - t_{i-1} e^{-.305t_{i-1}})}{e^{-.305t_{i-1}} - e^{-.305t_i}} - \frac{y_3 t_3 e^{-.305t_3}}{1 - e^{-.305t_3}}$$

$$= \frac{2(e^{-.305})}{1 - e^{-.305}} + \frac{2(2e^{-.610} - e^{-.305})}{e^{-.305} - e^{-.610}} + \frac{1(3e^{-.915} - 2e^{-.610})}{e^{-.610} - e^{-.915}}$$

$$- \frac{5 \cdot 3 \cdot e^{-.915}}{(1 - e^{-.915})}$$

$$= 10.04088223 - 10.04087226 = 9.96719302759 \times 10^{-6}$$

$$\frac{dF}{db} = \sum_{i=1}^{3} (y_i - y_{i-1}) \left[ \frac{(e^{-.305t_{i-1}} - e^{-.305t_i})(t_{i-1}^2 e^{-.305t_{i-1}} - t_i^2 e^{-.305t_i})}{(e^{-.305t_{i-1}} - e^{-.305t_i})^2} \right.$$

$$\left. - \frac{(t_i e^{-.305t_i} - t_{i-1} e^{-.305t_{i-1}})^2}{(e^{-.305t_{i-1}} - e^{-.305t_i})^2} \right] + \frac{y_3 t_3^2 e^{-.305t_3}}{(1 - e^{-.305t_3})^2}$$

$$= \frac{2[(1 - e^{-.305})(-e^{-.305}) - e^{-.610}]}{(1 - e^{-.305})^2} +$$

$$+ \frac{2[(e^{-.305} - e^{-.610})(e^{-.305} - 4e^{-.610}) - (2e^{-.610} - e^{-.305})^2]}{(e^{-.305} - e^{-.610})^2}$$

$$+ \frac{1[(e^{-.610} - e^{-.915})(4e^{-.610} - 9e^{-.915}) - (3e^{-.915} - 2e^{-.610})^2]}{(e^{-.610} - e^{-.915})^2}$$

$$+ \frac{45 \cdot e^{-.915}}{(1 - e^{-.915})^2}$$

$$= -\left( \frac{2e^{-.305}}{(1 - e^{-.305})^2} + \frac{2e^{-.915}}{(e^{-.305} - e^{-.610})^2} + \frac{e^{-1.525}}{(e^{-.610} - e^{-.915})^2} \right)$$

$$+ \frac{45e^{-.915}}{(1 - e^{-.915})^2}$$

$$= -53.470157 + 50.28643996 = -3.18371704092$$

$$\Delta b^{(3)} = -F \div dF/db = -9.96719302759 \times 10^{-6} \div -3.18371704092$$

$$= 3.1306781 \times 10^{-6}$$

Since $\Delta b^{(3)} < \epsilon$ (0.0001), we terminate further iterations.

Computation of $\hat{a}$ and $\hat{b}$

Since we met the criteria for $\Delta b^{(3)} < \epsilon$ (0.0001) we do not have to compute additional iterations, and we can compute $\hat{a}$ and $\hat{b}$ as follows:

$$\hat{b} = b^{(3)} + \Delta b^{(3)} = 3.0461826104 \times 10^{-1}$$

and

$$\hat{a} = \frac{y_3}{(1 - e^{-\hat{b}t_3})} = \frac{5}{(1 - e^{-.30461826104 \times 3})} = 8.346957421$$

Thus, for this data set

$$\hat{a} = 8.34695742$$
$$\hat{b} = 3.0461826104 \times 10^{-1}$$

After estimation of the parameters a and b the next step is to obtain performance measures as follows:

The expected number of faults detected by time t, $E[\hat{N}(t)]$, is obtained using the following formula:

$$E[\hat{N}(t)] = \hat{a}(1 - e^{-bt})$$

Let t=10. Substituting values for $\hat{a}$, $\hat{b}$, and t in the above formula we get

$$\begin{aligned} E[\hat{N}(10)] &= 8.34695742 \times (1 - e^{-3.0461826104 \times 10^{-1} \times 10}) \\ &= 7.950397851 \end{aligned}$$

The expected number of remaining faults by time t, $E[\hat{N}(t)]$, is obtained using the following formula:

$$E[\hat{\bar{N}}(t)] = \hat{a}e^{-\hat{b}t}$$

Let t=10. Substituting values for $\hat{a}$, $\hat{b}$, and t in the above formula we get

$$\begin{aligned} E[\hat{\bar{N}}(10)] &= 8.3469742 \times (e^{-3.0461826104 \times 10^{-1} \times 10}) \\ &= 8.34695742 \times e^{-3.0461826104} \\ &= 0.3965595689 \end{aligned}$$

The reliability at time t after nth testing interval, $\hat{R}_n(t)$, is obtained from the following formula:

$$\hat{R}_n(t) = \exp[-\hat{a}\{\exp[-\hat{b}xn] - \exp[\hat{b}x(n+t)]\}]$$

For the above example n=3. Let t be 1. After substituting values $\hat{a}$, $\hat{b}$, n, and t in the above formula we get

$$\begin{aligned} \hat{R}_3(1) = \exp[-8.34695742 \times \{\exp[-0.30461826104 \times 3] \\ - \exp[-0.30461826104 \times (3+1)]\} = 0.4152494843 \end{aligned}$$

The MTTF after nth testing interval, $\hat{MTTF}_n$, is obtained using the following formula:

$$\hat{MTTF}_n = \frac{1}{\hat{\lambda}(n)} = \frac{1}{\hat{a}\hat{b}\exp[-\hat{b}xn]}$$

For the above example n=3 and substituting values for $\hat{a}$ and $\hat{b}$ in the above formula we get

$$\hat{MTTF}_3 = \frac{1}{8.34695742 \text{ x } 0.30461826104 \text{ x } \exp[-0.30461826104 \text{ x } 3]}$$

$$= .9808216948$$

# APPENDIX D - WORKED EXAMPLE SHOWING COMPUTATIONS FOR THE JELINSKI-MORANDA DE-EUTROPHICATION MODEL

Worked example showing computations for the Jelinski-Moranda De-Eutrophication Model (Time Between Failures). This example has been adapted from Goel (1983).

Consider a set of failure times as follows:

| Failure No. | Time Between Failure $t_i$ |
|---|---|
| 1 | 3 |
| 2 | 30 |
| 3 | 113 |
| 4 | 31 |
| 5 | 115 |

The parameters to be estimated are N and Φ, where N is the total number of initial errors in the program; and Φ is a proportionality constant.

The maximum likelihood estimate (MLE) of N can be obtained from the following equation using the Newton-Raphson method:

$$\sum_{i=1}^{n} \frac{1}{N-(i-1)} - \frac{n}{N - \frac{1}{\sum_{i=1}^{n} t_i}\left(\sum_{i=1}^{n} (i-1)t_i\right)} = 0$$

Therefore, we can use the Newton-Raphson method to find $\hat{N}$ as follows:

$$F = \sum_{i=1}^{n} \frac{1}{N-(i-1)} - \frac{n}{N - \frac{1}{\sum_{i=1}^{n} t_i}\left(\sum_{i=1}^{n} (i-1)t_i\right)}$$

then

$$\frac{dF}{dN} \equiv \frac{n}{\left\{N - \frac{1}{\sum_{i=1}^{n} t_i}\left(\sum_{i=1}^{n} (i-1)\,t_i\right)\right\}^2} - \sum_{i=1}^{n} \frac{1}{\{N-(i-1)\}^2}$$

We can then find $\hat{\Phi}$ from the follcwing equation by substituting $\hat{N}$ for N

$$\hat{\Phi} = \frac{n}{\hat{N}\left(\sum_{i=1}^{n} t_i\right) - \sum_{i=1}^{n} (i-1)t_i}$$

For the above data set

$$\sum_{i=1}^{n} (i-1)t_i = \sum_{i=1}^{5} (i-1)t_i = t_2 + 2t_3 + 3t_4 + 4t_5$$

$$= 30 + 226 + 93 + 460 = 809$$

The computation of MLE to estimate $\hat{N}$ and $\hat{\Phi}$ is as follows:

Iteration 1. Let an initial value of $N^{(1)} = 5$

$$\text{Then } F^{(1)} = \sum_{i=1}^{5} \frac{1}{5 - i + 1} - \frac{5}{5 - \frac{1}{292} \cdot (809)}$$

$$= \left( \frac{1}{5} + \frac{1}{4} + \frac{1}{3} + \frac{1}{2} + 1 \right) - \frac{5}{2.229452055}$$

$$= 2.283333333 - 2.242703532$$

$$= 4.062980 \times 10^{-2}$$

and

$$\frac{dF^{(1)}}{dN^{(1)}} = \frac{5}{\{5 - \frac{1}{292}(809)\}^2} - \sum_{i=1}^{5} \frac{1}{\{5 - i + 1\}^2}$$

$$= \frac{5}{\{2.229452055\}^2} - \left( \frac{1}{25} + \frac{1}{16} + \frac{1}{9} + \frac{1}{4} + 1 \right)$$

$$\text{or } \frac{dF^{(1)}}{dN^{(1)}} = -4.57667284 \times 10^{-1}$$

Next

$$\Delta N^{(1)} = -F^{(1)} \div \frac{dF^{(1)}}{dN^{(1)}} = (4.062980 \times 10^{-2}) \div (4.57667284 \times 10^{-1})$$

$$= 0.0887758460?$$

Let error $\epsilon \leq 10^{-4}$. Since $\Delta N^{(1)} \not< 10^{-4}$, we go through the next iteration.

Iteration 2. The value of N for the second iteration is

$$N^{(2)} = N^{(1)} + \Delta N^{(1)} = 5.08877584602$$

$$F^{(2)} = \sum_{i=1}^{5} \frac{1}{5.08877584602 - i + 1} - \frac{5}{5.08877584602 - \frac{809}{292}}$$

$$\text{or } F^{(2)} = 5.22788908141 \text{ x } 10^{-3}$$

and

$$\frac{dF^{(2)}}{dN^{(2)}} = \frac{5}{\{5.08877584602 - \frac{809}{292}\}^2} - \sum_{i=1}^{5} \frac{1}{\{5.08877584602 - i + 1\}^2}$$

$$= .9303743904 - 1.276022534 = -3.45648143667 \times 10^{-1}$$

Now

$$\Delta N^{(2)} = -F^{(2)} \div \frac{dF^{(2)}}{dN^{(2)}} = (5.22788908141 \times 10^{-3}) \div (3.45648143667 \times 10^{-1})$$

$$= 0.0151248869$$

Since this number is > $10^{-4}$, we go to the next iteration.

Iteration 3. The value of N for the third iteration is

$$N^{(3)} = N^{(2)} + \Delta N^{(2)} = 5.08877584602 + 0.0151248869$$

$$= 5.10390073293$$

$$F^{(3)} = \sum_{i=1}^{5} \frac{1}{5.10390073293 - i + 1} - \frac{5}{5.10390073293 - \frac{809}{292}}$$

$$= 2.142960589 - 2.142839277 = 1.21312176929 \times 10^{-4}$$

and

$$\frac{dF^{(3)}}{dN^{(3)}} = \frac{5}{\{5.10390073293 - \frac{809}{292}\}^2} - \sum_{i=1}^{5} \frac{1}{\{5.10390073293 - i + 1\}^2}$$

$$= .9183520332 - 1.248093532 = -3.29741499203 \times 10^{-1}$$

$$\Delta N^{(3)} = -F^{(3)} \div \frac{dF^{(3)}}{dN^{(3)}} = (1.21312176929 \times 10^{-3}) \div (3.29741499203 \times 10^{-1})$$

$$= 3.679008472 \times 10^{-4}$$

Since $\Delta N^{(3)} > 10^{-4}$, we continue the computations.

Iteration 4. The value of N for the iteration is

$$N^{(4)} = N^{(3)} + \Delta N^{(3)} = 5.10390073293 + 3.679008472 \times 10^{-4}$$

$$= 5.10426863377$$

$$F^{(4)} = \sum_{i=1}^{5} \frac{1}{5.10426863377 - i + 1} - \frac{5}{5.10426863377 - \frac{809}{292}}$$

$$= 2.142501537 - .142501468 = 6.93541917229 \times 10^{-8}$$

$$\frac{dF^{(4)}}{dN^{(4)}} = \frac{5}{\{5.10426863377 - \frac{809}{292}\}^2} - \sum_{i=1}^{5} \frac{1}{\{5.10426863377 - i + 1\}^2}$$

$$= 0.9180625077 - 1.247427058 = -3.29364549966 \times 10^{-1}$$

and

$$\Delta N^{(4)} = -F^{(4)} \div \frac{dF^{(4)}}{dN^{(4)}} = (6.9354191722 \times 10^{-8}) \div (3.29364549966 \times 10^{-1})$$

$$= 2.105696916 \times 10^{-7}$$

Since $\Delta N^{(4)} < 10^{-4}$, we terminate further iterations.

Since we met the criteria for $\Delta N^{(4)} \leq 10^{-4}$, we do not have to compute additional iterations, and we can compute $\hat{N}$ and $\hat{\Phi}$ as follows:

$$\hat{N} = N^{(4)} + \Delta N^{(4)}$$

$$= 5.10426863377 + 2.105696916 \times 10^{-7}$$

or

$$\hat{N} = 5.104268844 \;\; ;$$

Using the above value of $\hat{N}$, we get

$$\hat{\Phi} = \frac{5}{5.104268844 \cdot \;(292) - 809}$$

$$= \frac{5}{1490.446502 - 809} = 5/681.446502$$

or

$$\hat{\Phi} = 7.337333131 \times 10^{-3}$$

Thus, for this data set, we get

$$\hat{N} = 5.104268844$$

$$\hat{\Phi} = 7.337333131 \times 10^{-3}$$

After estimating the parameters $\hat{N}$ and $\hat{\Phi}$, we calculate the performance measures using these estimates as follows:

The reliability at time t after nth failure, $\hat{R}_n(t)$, is obtained using the following formula:

$$\hat{R}_n(t) = \exp[-\hat{\Phi}(\hat{N} - n)t]$$

Let t=10. Substituting values for $\hat{N}$, $\hat{\Phi}$, n, and t in the above formula we get

$$\hat{R}_5(10) = \exp[-7.337333131 \times 10^{-3} \times (5.104268844 - 5) \times 10]$$

$$= .9923786386$$

The MTTF after nth failure, $M\hat{T}TF_n$, is obtained using the following formula:

$$M\hat{T}TF_n = \frac{1}{\hat{\Phi}(\hat{N} - n)}$$

Substituting values for $\hat{N}$, $\hat{\Phi}$, and n in the above formula we get

$$M\hat{T}TF_5 = \frac{1}{7.33733131 \times 10^{-3} \times (5.104268844 - 5)}$$

$$= 1307.095152$$

## APPENDIX E - WORKED EXAMPLES FOR THE N-VERSION SOFTWARE RELIABILITY DESIGN TECHNIQUES

Appendix E contains three worked examples using NVS reliability design techniques.

Example 1: Analysis of a system with NVS whose outputs go into a decision algorithm.

Example 2: Analysis of a system with NVS whose outputs are submitted to an acceptance test, and the outputs from the acceptance test are input to the decision algorithm.

Example 3: Analysis of a hybrid NVS which makes use of acceptance test, decision algorithm, and rollback.

Example 1:

Using the block diagram shown in figure E-1, a system with NVS whose outputs go into a decision algorithm will be analyzed. For this example, NVS will consist of five versions. The reliability values for the five versions and the decision algorithm are given in table E-1.

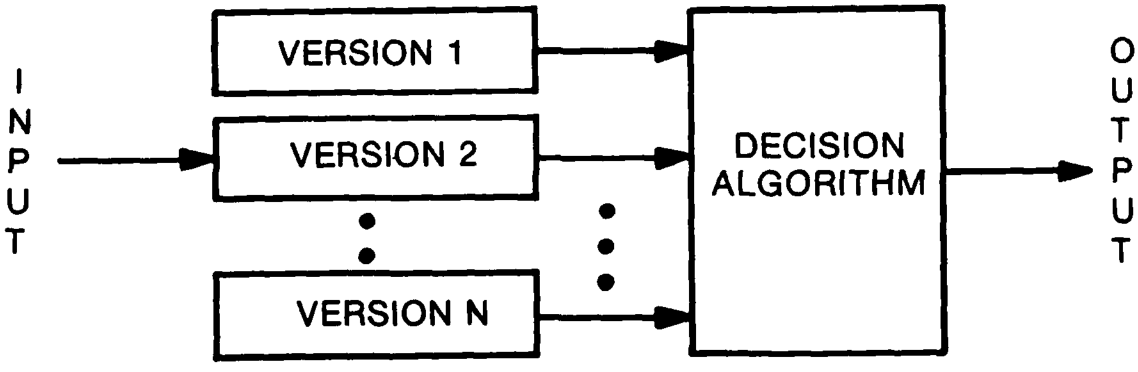


FIGURE E-1. GENERAL FORMAT FOR N-VERSION SOFTWARE

TABLE E-1. RELIABILITY VALUES FOR THE SOFTWARE COMPONENTS IN FIGURE E-1

| Software Component | Reliability Value |
|---|---|
| Version 1 | 0.77 |
| Version 2 | 0.82 |
| Version 3 | 0.65 |
| Version 4 | 0.91 |
| Version 5 | 0.89 |
| Decision Algorithm | 0.997 |

To determine the overall software reliability value for this block diagram, the transfer function for the NVS, which is dependent upon the number of versions (in this example n = 5), must first be determined. Hence, the transfer function for the NVS is

$$\begin{aligned} NVS = [1 - &(1-G_1G_2G_3)(1-G_1G_2G_4)(1-G_1G_2G_5)(1-G_1G_3G_4)(1-G_1G_3G_5) \times \\ &(1-G_1G_4G_5)(1-G_2G_3G_4)(1-G_2G_3G_5)(1-G_2G_4G_5)(1-G_3G_4G_5)] \end{aligned}$$

By substituting in the appropriate reliability values,

$$\begin{aligned} NVS = 1 - &[1-(0.77)(0.82)(0.65)][1-(0.77)(0.82)(0.91)] \times \\ &[1-(0.77)(0.82)(0.89)][1-(0.77)(0.65)(0.91)] \times \\ &[1-(0.77)(0.65)(0.89)][1-(0.77)(0.91)(0.89)] \times \\ &[1-(0.82)(0.65)(0.91)][1-(0.82)(0.65)(0.89)] \times \\ &[1-(0.82)(0.91)(0.89)][1-(0.65)(0.91)(0.89)] \end{aligned}$$

$$\begin{aligned} = [1 - &(1-0.41041)(1-0.574574)(1-0.561946)(1-0.455455) \times \\ &(1-0.445445)(1-0.623623)(1-0.48503)(1-0.47437) \times \\ &(1-0.664118)(1-0.526435)] \end{aligned}$$

$$\begin{aligned} = [1 - &(0.58959)(0.425426)(0.438054)(0.544545)(0.554555) \times \\ &(0.376377)(0.51497)(0.52563)(0.335882)(0.473565)] \end{aligned}$$

$$= 1 - 0.0005377 = 0.9994623$$

$$NVS = 0.99946$$

By applying the software reliability model,

$L_1$ through $L_n = 0$

$G_1 = (0.99946) \times (0.997) = 0.9964616$

$G_2$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta = 1$

Therefore,

$$\text{Reliability} = \frac{(0.9964616) \times (1)}{(1)} = 0.9964616$$

Reliability = 0.996

The probability of coincident errors (E) should be determined and subtracted from the transfer function for the NVS to improve the accuracy of the reliability value of the NVS and the accuracy of the overall software reliability value. For this example,

$$E = \binom{5}{3}^* (1-G_L)^3 + \binom{5}{4}^* (1-G_L)^4 + \binom{5}{5}^* (1-G_L)^5$$

The groups for $\binom{5}{3}^*$ would be

$G_1G_2G_3$, $G_1G_2G_4$, $G_1G_2G_5$, $G_1G_3G_4$, $G_1G_3G_5$, $G_1G_4G_5$, $G_2G_3G_4$, $G_2G_3G_5$, $G_2G_4G_5$, and $G_3G_4G_5$,

with respective $G_L$ values being

$G_2$, $G_4$, $G_5$, $G_4$, $G_5$, $G_4$, $G_4$, $G_5$, $G_4$, and $G_4$.

The $G_L$ values can be grouped as $G_2 + (6 \times G_4) + (3 \times G_5)$.

The groups for $\binom{5}{4}^*$ would be

$G_1G_2G_3G_4$, $G_1G_2G_3G_5$, $G_1G_2G_4G_5$, $G_1G_3G_4G_5$, and $G_2G_3G_4G_5$,

with the respective $G_L$ values being $G_4$, $G_5$, $G_4$, $G_4$, and $G_4$, giving

$4 \times G_4 + G_5$.

The group for $\binom{5}{5}^*$ is $G_1G_2G_3G_4G_5$ with $G_L = G_4$.

Therefore,

$$E = (1-G_2)^3 + 6 \times (1-G_4)^3 + 3 \times (1-G_5)^3 + 4 \times (1-G_4)^4 + (1-G_5)^4 + (1-G_4)^5$$

$$= (1-0.82)^3 + 6 \times (1-0.91)^3 + 3 \times (1-0.89)^3 + 4 \times (1-0.91)^4 + (1-0.89)^4 + (1-0.91)^5$$

$$= (0.18)^3 + 6 \times (0.09)^3 + 3 \times (0.11)^3 + 4 \times (0.09)^4 + (0.11)^4 + (0.09)^5$$

$$= 0.005832 + 0.004374 + 0.003993 + 0.0002624 + 0.0001464 + 0.0000059$$

$$E = 0.0146137$$

Subtracting E from the transfer function for the NVS gives

$$NVS = 0.9994623 - 0.0146137 = 0.9848486$$

$$NVS = 0.98485$$

$L_1$ through $L_n = 0$

$G_1 = (0.98485) \times (0.997) = 0.9818955$

$G_2$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta = 1$

Hence, the adjusted reliability value is

$$\text{Reliability} = \frac{(0.9818955) \times (1)}{(1)} = 0.9818955$$

$$\text{Reliability} = 0.982$$

Example 2:

This example will evaluate the overall reliability for the system shown in figure E-2. In this example, the NVS will consist of four versions. Each of the outputs from the NVS are submitted to an acceptance test (the identical acceptance test is used for all four versions), and then the outputs from the acceptance test are input to the decision algorithm. The reliability values for each of the software components are given in table E-2.

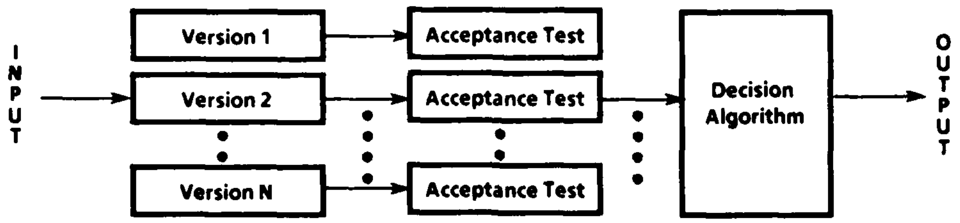


FIGURE E-2. N-VERSION SOFTWARE WITH ACCEPTANCE TESTS

TABLE E-2. RELIABILITY VALUES FOR THE SOFTWARE COMPONENTS IN FIGURE E-2

| Software Component | Reliability Value |
|---|---|
| Version 1 | 0.86 |
| Version 2 | 0.79 |
| Version 3 | 0.94 |
| Version 4 | 0.68 |
| Acceptance Test | 0.98 |
| Decision Algorithm | 0.93 |

First, the transfer function for the NVS must be determined. In this example,

$$NVS = [1 - (1-G_1G_2G_3)(1-G_1G_3G_4)(1-G_1G_2G_4)(1-G_2G_3G_4)].$$

By substituting in the appropriate reliability values,

$$\begin{aligned} NVS &= \{1 - [1 - (0.86)(0.79)(0.94)][1 - (0.86)(0.94)(0.68)] \times \\ &\quad [1 - (0.86)(0.79)(0.68)][1 - (0.79)(0.94)(0.68)]\} \\ &= [1 - (1-0.638636)(1-0.549712)(1-0.461992)(1-0.504968)] \\ &= [1 - (0.361364)(0.450288)(0.538008)(0.495032)] \\ &= 1 - 0.0433368 = 0.9566632 \end{aligned}$$

$$NVS = 0.95666$$

By applying the software reliability model,

$L_1$ through $L_n = 0$

$G_1 = (0.95666) \times (0.98) \times (0.93) = 0.8718999$

$G_2$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta = 1$

Therefore,

$$\text{Reliability} = \frac{(0.8718999) \times (1)}{(1)} = 0.8718999$$

$$\text{Reliability} = 0.872$$

The probability of coincident errors (E) for this example is

$$E = \binom{4}{2}^* \quad (1-G_L)^2 + \binom{4}{3}^* \quad (1-G_L)^3 + \binom{4}{4}^* \quad (1-G_L)^4$$

The groups for $\binom{4}{2}^*$ are

$G_1G_2$, $G_1G_3$, $G_1G_4$, $G_2G_3$, $G_2G_4$, and $G_3G_4$.

Their respective $G_L$ values are $G_1$, $G_3$, $G_1$, $G_3$, $G_2$, and $G_3$. These values can be grouped as $(2 \times G_1) + (2 \times G_2) + (2 \times G_3)$.

The groups for $\binom{4}{3}^*$ are $G_1G_2G_3$, $G_1G_2G_4$, $G_1G_3G_4$, and $G_2G_3G_4$, with the $G_L$ values $G_3$, $G_1$, $G_3$, and $G_3$, respectively, giving $G_1 + (3 \times G_3)$.

The group for $\binom{4}{4}^*$ 4 is $G_1G_2G_3G_4$ with $G_L = G_3$.

Hence,

$$E = 2 \times (1-G_1)^2 + 2 \times (1-G_2)^2 + 2 \times (1-G_3)^2 + (1-G_1)^3 + 3 \times (1-G_3)^3 + (1-G_3)^4$$

$$= 2 \times (1-0.86)^2 + 2 \times (1-0.79)^2 + 2 \times (1-0.94)^2 + (1-0.86)^3 + 3 \times (1-0.94)^3 + (1-0.94)^4$$

$$= 2 \times (0.14)^2 + 2 \times (0.21)^2 + 2 \times (0.06)^2 + (0.14)^3 + 3 \times (0.06)^3 + (0.06)^4$$

$$= 0.0392 + 0.0882 + 0.0072 + 0.002744 + 0.000648 + 0.00001296$$

$$E = 0.1380049$$

Re-evaluating the reliability value for the NVS and the overall software reliability value gives

$NVS = 0.9566632 - 0.00001296 = 0.9566503$

$NVS = 0.95665$

$L_1$ through $L_n = 0$

$G_1 = (0.95665) \times (0.98) \times (0.93) = 0.8718908$

$G_2$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta = 1$

Therefore, the adjusted reliability value is

$$\text{Reliability} = \frac{0.8718908 \times 1}{1} = 0.8718908$$

$$\text{Reliability} = 0.872$$

Example 3:

The hybrid NVS format, shown in figure E-3, will be evaluated in this example. The NVS here consists of three versions. The outputs of these versions are fed into a decision algorithm. If the decision algorithm fails, then the software will rollback and run through the three versions again. However, this time the outputs of the versions are input to an acceptance test prior to entry to the decision algorithm. For this example, it is assumed that the reliability values for the individual software components are as given in table E-3.

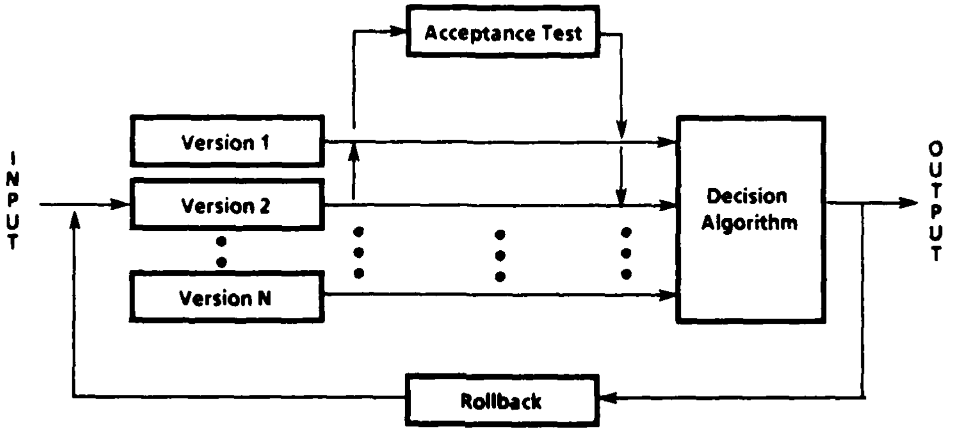


FIGURE E-3. N-VERSION SOFTWARE IN WHICH THE OUTPUTS ARE SUBJECTED TO AN ACCEPTANCE TEST IF THE DECISION ALGORITHM FAILS (Scott)

TABLE E-3. RELIABILITY VALUES FOR THE SOFTWARE COMPONENTS IN FIGURE E-3

| Software Component | Reliability Value |
|---|---|
| Version 1 | 0.67 |
| Version 2 | 0.78 |
| Version 3 | 0.89 |
| Acceptance Test | 0.86 |
| Decision Algorithm | 0.88 |
| Rollback | 0.98 |

The transfer function for the NVS, based on the data in table E-3, is

$$NVS = 1-(1-G_1G_2)(1-G_1G_3)(1-G_2G_3)$$

$$= 1-[1-(0.67)(0.78)][1-(0.67)(0.89)][1-(0.78)(0.89)]$$

$$= 1-(1-0.5226)(1-0.5963)(1-0.6942)$$

$$= 1-(0.4774)(0.4037)(0.3058)$$

$$NVS = 0.94106428$$

The variables of the software reliability model are

$$\text{Closed Loop \#1} = (0.94106428) \times (0.88) \times (1-0.98)$$

$$= 0.01656273$$

$$\text{Closed Loop \#2} = (0.94106428) \times (1-0.86) \times (0.88) \times (1-0.98)$$

$$= 0.0023187824$$

[Remember that the transfer function of the equivalent block in a feedback or feed-forward path is (1.0 - reliability value).]

$$\Sigma L_1 = \text{Closed Loop \#1} + \text{Closed Loop \#2} = 0.018881512$$

$$\Sigma L_2 \text{ through } \Sigma L_n = 0$$

$$G_1 = (0.94106428) \times (0.88) = 0.82813657$$

$$G_2 = (0.94106428) \times (1-0.86) \times (0.88) = 0.11593912$$

$$G_3 \text{ through } G_K = 0$$

$$\Delta_1 = 1$$

$$\Delta_2 = 1$$

$$\Delta_3 \text{ through } \Delta_K = 0$$

$$\Delta = 1 - \Sigma L_1 = 1 - 0.018881512 = 0.981118488$$

Therefore,

$$\text{Reliability} = \frac{(0.82813657 \times 1) + (0.11593912 \times 1)}{(0.981118408)} = 0.9622444$$

$$\text{Reliability} = 0.962$$

To improve the accuracy of the software reliability model, the probability of coincident errors (E) might be considered. For this example,

$$E = \binom{3}{2}^* \quad (1\text{-}GL)^2 + \binom{3}{3}^* \quad (1\text{-}GL)^3$$

The groups for $\binom{3}{2}^*$ are $G_1G_2$, $G_1G_3$, and $G_2G_3$ with respective $G_L$ values of $G_2$, $G_3$, and $G_3$, or $G_2 + (2 \times G_3)$. The group for $\binom{3}{3}^*$ is $G_1G_2G_3$ with $G_L = G_3$.

Thus,

$$E = (1\text{-}G_2)^2 + 2 \times (1\text{-}G_3)^2 + (1\text{-}G_3)^3$$

$$= (1\text{-}0.78)^2 + 2 \times (1\text{-}0.89)^2 + (1\text{-}0.89)^3$$

$$= (0.22)^2 + 2 \times (0.11)^2 + (0.11)^3$$

$$= 0.0484 + 0.0242 + 0.001331$$

$$E = 0.073931$$

By subtracting the probability of coincident errors from the NVS transfer function, a conservative value of the reliability value for the NVS and the overall software reliability value can be determined.

NVS = 0.94106428 - 0.073931 = 0.86713328

Closed Loop #1 = (0.86713328) x (0.88) x (1-0.98)

= 0.015261546

Closed Loop #2 = (0.86713328) x (1-0.86) x (0.88) x (1-0.98)

= 0.0021366164

$\Sigma L_1$ = 0.015261546 + 0.0021366164 = 0.017398162

$\Sigma L_2$ through $\Sigma L_n$ = 0

$G_1$ = (0.86713328) x (0.88) = 0.76307729

$G_2$ = (0.86713328) x (1-0.86) x (0.88) = 0.10683082

$G_3$ through $G_K$ = 0

$\Delta_1$ = 1

$\Delta_2 = 1$

$\Delta_3$ through $\Delta_K = 0$

$\Delta = 1 - \Sigma L_1 = 1 - 0.017398162 = 0.98260184$

Therefore,

$$\text{Reliability} = \frac{(0.76307729 \times 1) + (0.10683082 \times 1)}{(0.98260184)} = 0.88531089$$

Reliability = 0.885

## APPENDIX F - WORKED EXAMPLES FOR THE RECOVERY BLOCK SOFTWARE RELIABILITY DESIGN TECHNIQUES

Appendix F contains three worked examples using RB software reliability design techniques.

Example 1: Analysis of a system which uses the general format of the backward RB.

Example 2: Analysis of a system which uses the general format of a forward RB.

Example 3: Analysis of a system which uses a variation of the forward RB format.

Example 1:

Figure F-1 shows the general format of a backward RB. For this example, the number of alternates will be four. The reliability value for each of the software components is listed in table F-1.

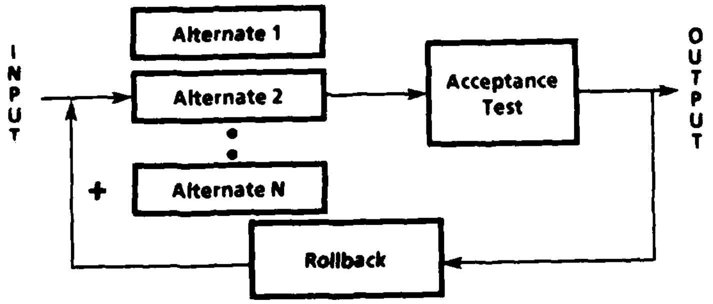


FIGURE F-1. GENERAL FORMAT OF A BACKWARD RECOVERY BLOCK

TABLE F-1. RELIABILITY VALUES FOR THE SOFTWARE COMPONENTS IN FIGURE F-1

| Software Component | Reliability Value |
|---|---|
| Alternate 1 | 0.86 |
| Alternate 2 | 0.75 |
| Alternate 3 | 0.79 |
| Alternate 4 | 0.84 |
| Acceptance Test | 0.91 |
| Rollback | 0.93 |

The transfer function for the RB is

$$\begin{aligned} RB &= G_1 + (1 - G_1)G_2 + (1 - G_1)(1 - G_2)G_3 + \\ &\quad (1 - G_1)(1 - G_2)(1 - G_3)\ G_4 \\ &= 0.86 + (1 - 0.86)(0.75) + (1 - 0.86)(1 - 0.75)(0.79) + \\ &\quad (1 - 0.86)(1 - 0.75)(1 - 0.79)(0.84) \\ &= 0.86 + (0.14)(0.75) + (0.14)(0.25)(0.79) + \\ &\quad (0.14)(0.25)(0.21)(0.84) \\ &= 0.86 + 0.105 + 0.02765 + 0.006174 \\ RB &= 0.998824 \end{aligned}$$

The variables of the software reliability model will be

$$L_1 = (0.998824) \times (0.91) \times (1.0 - 0.93) = 0.0636251$$

[Recall that the transfer function for rollback is (1.0 - reliability value).]

$$L_2 \text{ through } L_n = 0$$

$$G_1 = (0.998824) \times (0.91) = 0.9089298$$

$$G_2 \text{ through } G_K = 0$$

$$\Delta_1 = 1$$

$\Delta_2$ through $\Delta_K = 0$

$\Delta = 1 - 0.0636251 = 0.9363749$

Therefore,

$$\text{Reliability} = \frac{(0.9089298) \times (1)}{(0.9363749)} = 0.9706901$$

Reliability = 0.97

If only two of the four possible alternatives are actually used, the reliability of the RB will decrease. The overall software reliability will also decrease. The following calculations show this:

$$\begin{aligned} RB &= G_1 + (1 - G_1)G_2 = 0.86 + (1 - 0.86)(0.75) \\ &= 0.86 + 0.105 = 0.965 \end{aligned}$$

$L_1 = (0.965) \times (0.91) \times (1 - 0.93) = 0.0614705$

$L_2$ through $L_n = 0$

$G_1 = (0.965) \times (0.91) = 0.9089298$

$G_2$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta_2$ through $\Delta_K = 0$

$\Delta = 1 - 0.0614705 = 0.9385295$

Hence,

$$\text{Reliability} = \frac{(0.9089298) \times (1)}{(0.9385295)} = 0.9684616$$

Reliability = 0.968

when only two of the alternates are used.

Example 2:

The general format of a forward RB is shown in figure F-2. This example will evaluate the overall software reliability of this figure (six alternatives will be used: one primary and five alternates), with the reliability values assigned as shown in table F-2.

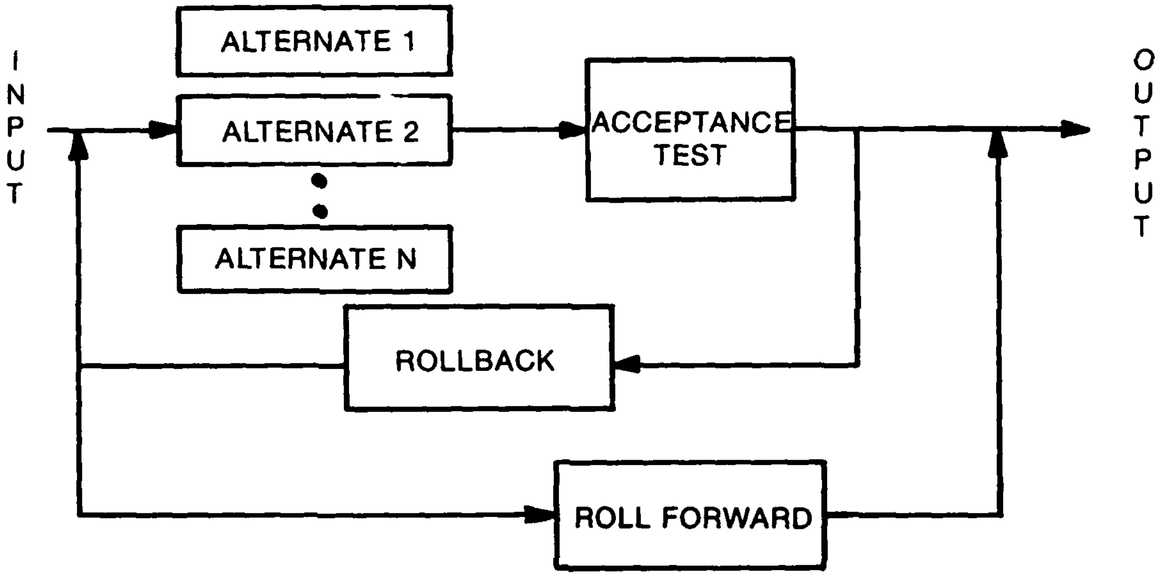


FIGURE F-2. GENERAL FORMAT OF A FORWARD RECOVERY BLOCK

TABLE F-2. RELIABILITY VALUES FOR THE SOFTWARE COMPONENTS IN FIGURE F-2

| Software Component | Reliability Value |
|---|---|
| Alternate 1 | 0.81 |
| Alternate 2 | 0.72 |
| Alternate 3 | 0.73 |
| Alternate 4 | 0.74 |
| Alternate 5 | 0.85 |
| Alternate 6 | 0.86 |
| Acceptance Test | 0.97 |
| Rollback | 0.98 |
| Roll-Forward | 0.89 |

The transfer function for the RB is

$$\begin{aligned} RB = {} & G_1 + (1 - G_1)G_2 + (1 - G_1)(1 - G_2)G_3 + \\ & (1 - G_1)(1 - G_2)(1 - G_3)G_4 + \\ & (1 - G_1)(1 - G_2)(1 - G_3)(1 - G_4)G_5 + \\ & (1 - G_1)(1 - G_2)(1 - G_3)(1 - G_4)(1 - G_5)G_6 \end{aligned}$$

$$\begin{aligned} = {} & 0.81 + (1 - 0.81)\ (0.72) + (1 - 0.81)(1 - 0.72)(0.73) + \\ & (1 - 0.81)(1 - 0.72)(1 - 0.73)(0.74) + \\ & (1 - 0.81)(1 - 0.72)(1 - 0.73)(1 - 0.74)(0.85)+ \\ & (1 - 0.81)(1 - 0.72)(1 - 0.73)(1 - 0.74)(1 - 0.85)(0.86) \end{aligned}$$

$$\begin{aligned} = {} & 0.81 + (0.19)(0.72) + (0.19)(0.28)(0.73) + \\ & (0.19)(0.28)(0.27)(0.74) + (0.19)(0.28)(0.27)(0.26)(0.85) + \\ & (0.19)(0.28)(0.27)(0.26)(0.15)(0.86) \end{aligned}$$

$$\begin{aligned} = {} & 0.81 + 0.1368 + 0.038836 + 0.01062936 + 0.003174444 + \\ & 0.00048176856 \end{aligned}$$

$$= 0.99992157256$$

$$RB = 0.9999216$$

With the software reliability model,

$$L_1 = (0.9999216) \times (0.97) \times (1 - 0.98) = 0.019398479$$

[Note that the transfer function for rollback is (1.0 - reliability value).]

$$L_2 \text{ through } L_n = 0$$

$$G_1 = (0.9999216) \times (0.97) = 0.96992395$$

$$G_2 = (0.9999216) \times (0.97) \times (1 - 0.98) \times (1 - 0.89) = 0.0021338327$$

[Remember that the transfer function for rollback and roll-forward is (1.0 - reliability value).]

$$G_3 \text{ through } G_K = 0$$

$$\Delta_1 = 1$$

$$\Delta_2 = 1$$

$$\Delta_3 \text{ through } \Delta_K = 0$$

$$\Delta = 1 - 0.019398479 = 0.98060152$$

Therefore,

$$\text{Reliability} = \frac{(0.96992395 \times 1) + (0.0021338327 \times 1)}{(0.98060152)}$$

$$= (0.97205778)/(0.98060152) = 0.99128725$$

$$\text{Reliability} = 0.991$$

Discussion of the Results

This result is as expected. With just the n alternates, acceptance test, and rollback, the overall reliability would be

$$\text{Reliability} = \frac{(0.9999216)(0.97)}{1 - (0.9999216)(0.97)(1 - 0.98)}$$

$$\text{Reliability} = 0.9891112 = 0.989$$

The roll-forward should increase this reliability value, as it does.

Alternative Calculations (Fewer than n alternatives)

To evaluate the effect on accuracy when fewer than the n alternates (in this example n = 6) are actually used, the reliability of this example will be evaluated with n = 3, n = 4, and n = 5.

For n = 3,

$$RB = G_1 + (1 - G_1)G_2 + (1 - G_1)(1 - G_2)G_3$$

$$= 0.81 + (1 - 0.81)(0.72) + (1 - 0.81)(1 - 0.72)(0.73)$$

$$= 0.81 + 0.1368 + 0.038836$$

$$RB = 0.985636$$

Using the software reliability model,

$$L_1 = (0.985636)(0.97)(1 - 0.98) = 0.019121338$$

$$L_2 \text{ through } L_n = 0$$

$$G_1 = (0.985636)(0.97) = 0.95606692$$

$$G_2 = (0.985636)(0.97)(1 - 0.98)(1 - 0.89) = 0.0021033472$$

$$G_3 \text{ through } G_K = 0$$

$\Delta_1 = 1$

$\Delta_2 = 1$

$\Delta_3$ through $\Delta_K = 0$

$\Delta = 1 - 0.019121338 = 0.98087866$

gives

$$\text{Reliability} = \frac{(0.95606692 \times 1) + (0.0021033472 \times 1)}{(0.98087866)} = 0.97684893$$

Reliability = 0.977

For $n = 4$,

$RB = 0.81 + 0.1368 + 0.038836 + 0.01062936$

$RB = 0.99626536$

Using the software reliability model,

$L_1 = (0.99626536)(0.97)(1 - 0.98) = 0.019327547$

$L_2$ through $L_n = 0$

$G_1 = (0.99626536)(0.97) = 0.9663774$

$G_2 = (0.99626536)(0.97)(1 - 0.98)(1 - 0.89) = 0.0021260303$

$G_3$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta_2 = 1$

$\Delta_3$ through $\Delta_K = 0$

$\Delta = 1 - 0.019327547 = 0.98067245$

gives

$$\text{Reliability} = \frac{(0.9663774 \times 1) + (0.0021260303 \times 1)}{(0.98067245)} = 0.98759115$$

Reliability = 0.988

For n = 5,

$$RB = 0.99626536 + 0.003174444$$

$$RB = 0.999439804$$

Using the software reliability model,

$$L_1 = (0.999439804)(0.97)(1 - 0.98) = 0.019389132$$

$$L_2 \text{ through } L_n = 0$$

$$G_1 = (0.999439804)(0.97) = 0.96945661$$

$$G_2 = (0.999439804)(0.97)(1 - 0.98)(1 - 0.89) = 0.0021328045$$

$$G_3 \text{ through } G_K = 0$$

$$\Delta_1 = 1$$

$$\Delta_2 = 1$$

$$\Delta_3 \text{ through } \Delta_K = 0$$

$$\Delta = 1 - 0.019389132 = 0.98061087$$

gives

$$\text{Reliability} = \frac{(0.96945661 \times 1) + (0.0021328045 \times 1)}{(0.98061087)} = 0.99080017$$

$$\text{Reliability} = 0.991$$

Discussion of the Results

Table F-3 compares the reliability values that are obtained by using fewer than n alternates in this example.

This is as expected. Actually using fewer than the n alternates, the reliability values for the RB and the overall software will generally decrease. However, as was seen in the case with n = 5, by not using the sixth alternate (which has a reliability value of 0.86 in this example), an extremely slight increase in reliability was found.

TABLE F-3. ACCURACY EFFECTS WHEN FEWER THAN n ALTERNATES ARE USED

| Number of Alternates Used | Recovery Block Reliability Value | Overall Software Reliability Value |
|---|---|---|
| n = 3 | 0.98564 | 0.977 |
| n = 4 | 0.99627 | 0.988 |
| n = 5 | 0.99944 | 0.991 |
| n = 6 | 0.99992 | 0.991 |

Example 3:

Figure F-3 shows a possible variation of a forward RB. For this example, the number of alternates will be three. The reliability value for each of the software components is listed in table F-4.

A variation of the forward RB format might be:

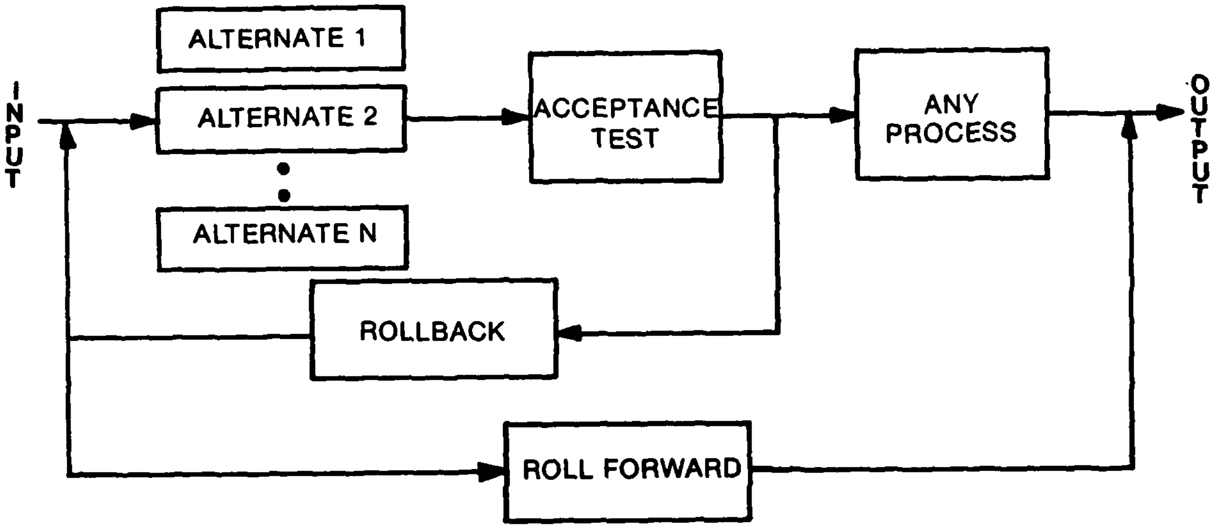


FIGURE F-3. ALTERNATE FORMAT FOR A FORWARD RECOVERY BLOCK

TABLE F-4. RELIABILITY VALUES FOR THE SOFTWARE COMPONENTS IN FIGURE F-3

| Software Component | Reliability Value |
|---|---|
| Alternate 1 | 0.80 |
| Alternate 2 | 0.70 |
| Alternate 3 | 0.90 |
| Acceptance Test | 0.98 |
| Any Process | 0.97 |
| Rollback | 0.95 |
| Roll-Forward | 0.96 |

The transfer function for the RB is

$$\begin{aligned} RB &= G_1 + (1 - G_1)G_2 + (1 - G_1)(1 - G_2)G_3 \\ &= 0.80 + (1 - 0.80) \times (0.70) + (1 - 0.80) \times (1 - 0.70) \times (0.90) \\ &= 0.80 + (0.20 \times 0.70) + (0.20 \times 0.30 \times 0.90) \\ &= 0.80 + 0.14 + 0.054 \end{aligned}$$

$$RB = 0.994$$

The variables of the software reliability model are

$$L_1 = (0.994) \times (0.98) \times (1 - 0.95) = 0.048706$$

$L_2$ through $L_n = 0$

$$G_1 = (0.994) \times (0.98) \times (0.97) = 0.9448964$$

$$G_2 = (0.994) \times (0.98) \times (1 - 0.95) \times (1 - 0.96) = 0.0019482$$

$G_3$ through $G_K = 0$

$$\Delta_1 = 1$$

$$\Delta_2 = 1$$

$\Delta_3$ through $\Delta_K = 0$

$$\Delta = 1 - L_1 = 1 - 0.048706 = 0.951294$$

Therefore,

$$\text{Reliability} = \frac{(0.9448964 \times 1) + (0.0019482 \times 1)}{(0.951294)} = 0.99532279$$

$$\text{Reliability} = 0.995$$

To demonstrate the effect on accuracy if fewer than the n alternates (in this example $n = 3$) are actually used, the reliability of the RB and overall software reliability value will be re-calculated for $n = 1$ and $n = 2$.

For $n = 1$, $RB = 0.80$

With the software reliability model,

$$L_1 = (0.80) \times (0.98) \times (1 - 0.95) = 0.0392$$

$L_2$ through $L_n = 0$

$G_1 = (0.80) \times (0.98) \times (0.97) = 0.76048$

$G_2 = (0.80) \times (0.98) \times (1 - 0.95) \times (1 - 0.96) = 0.001568$

$G_3$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta_2 = 1$

$\Delta_3$ through $\Delta_K = 0$

$\Delta = 1 - L_1 = 1 - 0.0392 = 0.9608$

$$\text{Reliability} = \frac{(0.76048 \times 1) + (0.001568 \times 1)}{(0.9608)} = 0.7931391$$

Reliability = 0.793

For n = 2, RB = 0.80 + 0.14 = 0.94

With the software reliability model,

$L_1 = (0.94) \times (0.98) \times (1 - 0.95) = 0.04606$

$L_2$ through $L_n = 0$

$G_1 = (0.94) \times (0.98) \times (0.97) = 0.893564$

$G_2 = (0.94) \times (0.98) \times (1 - 0.95) \times (1 - 0.96) = 0.0018424$

$G_3$ through $G_K = 0$

$\Delta_1 = 1$

$\Delta_2 = 1$

$\Delta_3$ through $\Delta_K = 0$

$\Delta = 1 - L_1 = 1 - 0.04606 = 0.95394$

$$\text{Reliability} = \frac{(0.893564 \times 1) + (0.0018424 \times 1)}{(0.95394)} = 0.93864017$$

Reliability = 0.939

## Discussion of the Results

Table F-5 compares the RB reliability values and the overall software reliability values that are obtained by using n or fewer than n alternates in this example.

TABLE F-5. COMPARISON OF RELIABILITY VALUES WHEN FEWER THAN n ALTERNATES ARE USED

| Number of Alternates Used | Recovery Block Reliability Value | Overall Software Reliability Value |
|---|---|---|
| n = 1 | 0.80 | 0.793 |
| n = 2 | 0.94 | 0.939 |
| n = 3 | 0.994 | 0.995 |

## BIBLIOGRAPHY

Anderson, T., and J. Knight, "Software Fault Tolerance for Real-Time Avionics Systems," AGARD Conference Proceedings No. 330, Software for Avionics, September 1982.

Eckhardt, D. E. Jr., and L. D. Lee, A Theoretical Basis for the Analysis of Redundant Software Subject to Coincident Errors, NASA Langley Research Center, NASA Technical Memorandum 86369, January 1985.

Gephart, L. S., et al., Software Reliability: Determination and Prediction, Technical Report AFFDL-TR-78-77, Air Force Flight Dynamics Laboratory, Air Force Systems Command, Wright-Patterson Air Force Base, OH, June 1978.

Goel, A. L., A Guidebook for Software Reliability Assessment, Technical Report RADC-TR-83-176 (AD A139240), Rome Air Development Center, Air Force Systems Command, Griffiss Air Force Base, NY, August 1983.

Hecht, H., "Fault-Tolerant Software," IEEE Transactions on Reliability, Vol. R-28, No. 3, pp. 227-232, August 1979.

Hitt, E. F., J. J. Webb, and M. S. Bridgman, Comparative Analysis of Fault-Tolerance Software Design Techniques, Prepared Under Contract Number NAS1-17412, February 15, 1984.

Krauson, S. S., and D. R. Baker, "Software Reliability Enhancement Techniques and Assessment Method for Embedded Computer Systems," IEEE 1982 National Aerospace and Electronics Conference, NAECON 1982, May 1982.

Larsen, W., et al., "An Overview of the Digital Avionics Assessment Activities Being Conducted by the Federal Aviation Administration at NASA-Ames Research Center," Proceedings of the AIAA/IEEE 6th Digital Avionics Systems Conference, December 1984.

Prater, S. A., E. F. Hitt, and D. Eldredge, Software Dependability Assessment Methods, DOT/FAA/CT-86/27, FAA Technical Center, Atlantic City Airport, NJ, November 1986.

Ramamoorthy, C. V., and F. B. Bastani, "Software Reliability - Status and Perspectives," IEEE Transactions on Software Engineering, Vol. SE-8, No. 4, 354-371, July 1982.

Scott, R. K., J. W. Gault, and D. F. McAllister, "Modeling Fault Tolerant Software Reliability," Proceedings of the Third Symposium on Reliability in Distributed Software and Database Systems, 1983.

Scott, R. K., J. W. Gault, and D. F. McAllister, "Fault Tolerant Software Reliability Modeling," IEEE Transactions on Software Engineering, 1987, Vol. SE-13, No. 5, pp. 582-592, May 1987.

__________, et al., "Investigating Version Dependence in Fault-Tolerant Software," AGARD Conference Proceedings No. 361, Design for Tactical Avionics Maintainability, May 1984.

Shinners, S. M., Modern Control System Theory and Application, Addison-Wesley Publishing Company, Inc., U.S.A., 1978.

Shooman, M. L., "Software Reliability: A Historical Perspective," IEEE Transactions on Reliability, Vol. R-33, No. 1, pp. 48-54, April 1984.

## GLOSSARY

ERROR. A state of the system which (in the absence of any corrective action by the system) could lead to a failure that would not be attributed to any event subsequent to the error. (More accurately known as an erroneous state.)

FAILURE. The situation when the external behavior of a system does not conform to that prescribed by the system specification.

FAULT. The adjusted cause of error.

HAZARD FUNCTION. The conditional probability that a fault is exposed in the interval t to Δt given that the fault did not occur prior to time t.

VOTING PROCEDURE. An algorithm included in fault tolerant software which uses the consensus RB method. It compares outputs of the n independent versions and determines which outputs are correct by identifying agreements among two or more versions.

## ACRONYMS AND ABBREVIATIONS

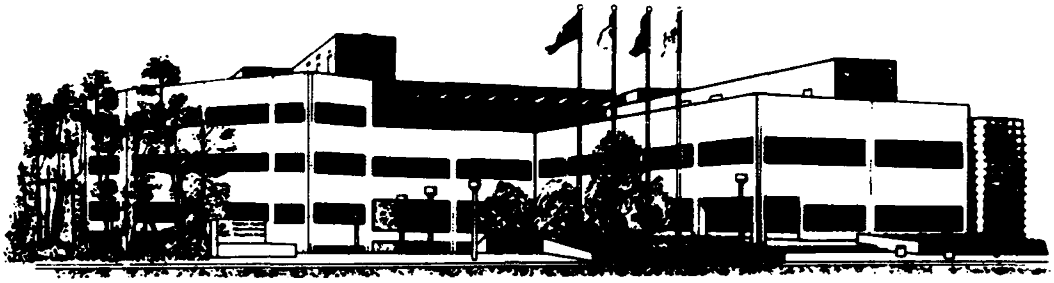
| | |
|---|---|
| AFFDL | Air Force Flight Dynamics Laboratory |
| AGARD | Advisory Group for Aerospace Research and Development |
| cdf | Cumulative Density Function |
| DOD | Department of Defense |
| DOT | Department of Transportation |
| FAA | Federal Aviation Administration |
| MLE | Maximum Likelihood Estimates |
| MTTF | Mean Time to Failure |
| NHPP | Non-Homogeneous Poisson Process |
| NVS | N-version Software |
| pdf | Probability Density Function |
| RADC | Rome Air Development Center |
| RB | Recovery Block |

S. Department of Transportation
Federal Aviation Administration

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 9
## FAULT TOLERANT SOFTWARE



PREPARED BY:

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

PREPARED FOR:

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

## TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

# 1. INTRODUCTION

As digital systems for flight control, engine control, power distribution, and other flight critical functions have increased in sophistication and complexity, the need for fault tolerant software to overcome software reliability problems has become more apparent. This chapter describes fault tolerant software techniques and concerns in certification and validation. Section 1 explains why traditional software development methods are inadequate and where the use of fault tolerant software is required. Sections 2 through 4 discuss the three major categories of software fault tolerance: partial fault tolerance, N-version software, and recovery blocks. Section 5 describes the tradeoffs and considerations in fault tolerant versus non-fault tolerant software, and section 6 discusses the combination and integration of several fault tolerance techniques.

## 1.1. Motivation for Fault Tolerant Software

At present, the most common approach for development of critical real-time software can be termed fault avoidance, i.e., attempting to prevent any software faults in the final delivered product through disciplined software development practices, testing, and Independent Verification and Validation (IV&V).

However, fault avoidance methods have their limitations. Most test methodologies used in verification do not have well-defined termination criteria; i.e., it is usually difficult to decide when enough testing has been performed. Investigations of software test strategies (Dijkstra, 1972, Howden, 1978, and Miller, 1981) have shown that fault densities of approximately 1 per 1000 lines of source code remain even after extensive testing. The limitations of testing were capsulized in the famous saying of E.W. Dijkstra, "Program testing can be used to show the presence of bugs but never their absence." IV&V limitations include:

- The program specification on which verification occurs is generally incomplete because it cannot include enough end-to-end test cases, exception conditions, and comprehensive run time attributes, such as response time or memory utilization.

- Hardware development is frequently conducted in parallel with the software development. IV&V activities are not carried out on the processors on which the operational code will be executed.

- Changes in the system requirements, environments, or the program itself result in the need to perform extensive retesting. The amount of regression testing necessary to ensure verification after changes is uncertain and is often dictated by cost or schedule rather than technical considerations.

Such limitations prompted the developers of Bell Laboratories' No. 4 ESS (Electronic Switching System) to conclude that it

> "...is not technically or economically feasible to detect and fix all software problems in a system as large as the No. 4 ESS. Consequently, a strong emphasis has been placed on making it sufficiently tolerant of software errors to provide successful operation and fault recovery in an environment containing software problems." (Davis and Giloth, 1981)

The No. 4 ESS program referred to in this quotation occupies slightly over two million words of computer memory. Although current flight control and management software is typically only half this size, increasing use of higher order languages, the advent of the "glass cockpit," fly-by-wire control systems, full authority digital engine controllers, and other trends point in the direction of increasing software size and complexity. As these applications become more sophisticated, the need for fault tolerance to achieve higher software reliability is correspondingly greater. However, fault tolerance provisions use resources; therefore, their practical use will require tradeoffs between the need for fault tolerance and the cost incurred by its implementation. Resource utilizations will usually consist of the following components:

- Software development: Staff resources required for the additional code plus corresponding increases in documentation and test.

- Performance penalty: Increase in execution time due to tests and alternate versions that have been incorporated in the program.

- Storage expansion: Additional memory required for storage of tests, alternate versions, alternate routines (for recovery blocks), and recovery cache provisions.

- Higher maintenance costs: Additional costs due to both the inherent increase in the amount of code and the need for increased testing after changes to ensure that the fault tolerance provisions are still intact.

Thus, it is impractical to apply fault tolerance provisions throughout the entire code. Instead, they should be confined to critical modules and components. Another technique to reduce the cost of fault tolerance provisions is to generate a highly "robust" kernel that can then be utilized to direct the error detection and exception handling in other segments of the program. This kernel would include fault tolerance provisions. The "nucleus" of this kernel would contain a small amount of very highly verified software that could be used for fault detection and recovery of other portions of the kernel which, in turn, would be responsible for recovery of the balance of the system.

The discussion of software fault tolerance techniques in the following sections proceeds in the order of increasing effectiveness and computing resource requirements. Only the most effective and therefore costly fault tolerance techniques should be utilized where a failure can cause complete termination of further program execution. Where failure can only cause faulty displays which will be readily recognized by the operator who has continued ability to call for the display of other screens, only the less costly measures will be considered.

## 2. PARTIAL SOFTWARE FAULT TOLERANCE TECHNIQUES

Partial software fault tolerance techniques have the capability to minimize rather than totally mask a fault. They detect and recover from faults without resorting to an alternate, redundant version of the function in order to produce an acceptable result. Thus, partial software fault toleran‿e techniques are nonredundant fault tolerance provisions. The two general classes are:

- Robustness: Substitution of an alternate value and continuation of execution if a software fault is detected.
- Rollback: Retrying the calculation in the event that a failure is detected, under the assumption that some external condition may have changed thereby resolving the anomaly.

### 2.1. Robustness

The Data Analysis Center for Software in Rome, New York, defined Robustness as the ability of the code to perform despite some violation of the assumptions in its specifications (DACS, March 1979). An example is the proper handling of out-of-range inputs without degrading the performance of functions not dependent on that input. Under such conditions, a new input may be requested (particularly if it can be supplied by a human operator), the last acceptable value can be used, or a predefined default can be assigned. In all cases, a program flag is set to notify the operator of a program exception state and to facilitate handling of the exception condition by other program elements.

Most of the techniques described as "self-checking" software are included in this definition. Self-checking features include (Yau and Cheung, 1975):

- Functionality: Range or reasonableness checks on the output.
- Control sequences: Setting an upper limit on loop iterations.
- Input data: Parity and type checks.

A distinctive feature of robustness is the protection it provides against predefined causes of software problems. An advantage of this specificity is that errors are usually detected before they can contaminate related programs or data sets. It can therefore be referred to as a technique of forward recovery. Robustness cannot usually be depended on to provide complete protection against faulty algorithms or implementations because of the possibility of faults for which no checks were incorporated.

## 2.2. Rollback

Rollback consists of the following three elements: an error detection mechanism, a protective action, and a recovery cache.

The recovery cache is the specific feature which distinguishes rollback from robustness. Error detection mechanisms can be input or output assertion checks, accounting tests, range checks, reasonableness tests, hardware alarms (e.g., divide by zero, overflow), and timeout interrupts. When the detection mechanism senses an exception condition, it usually sets a flag to notify the operator and to facilitate handling of the exception condition by using other programs. The usual protective actions are rollback to the beginning of the affected module or restart of the entire program. The recovery cache contains the data necessary for reexecution of the program or segment. During execution the program writes to a temporary memory section. The newly written values are accepted as permanent, replacing those in the recovery cache after the program has passed all checks. This methodology also prevents failures in one section of the code from contaminating other data. For these reasons, rollback has also been referred to as fault containment (Hecht and Hecht, 1986).

Rollback is effective when the failure is triggered by a temporary and unusual data value or computer control state. As the name implies, it is primarily aimed at limiting the propagation of faulty data. Rollback is a broader technique than robustness, but it does not always assure that the program will continue to run after an error has been detected. If the failure-inducing condition is short lived, the program can be expected to resume normal operation after a rollback or restart or in the next iteration. However, if the condition persists, the restoration of service will not be immediate or automatic. Because the technique depends on a recovery cache, it is a backward recovery technique.

## 2.3. Issues in Partial Fault Tolerance

Three issues to consider in the course of certification of partial fault tolerance provisions for flight critical systems are verification, performance, and coverage.

One concern of verification of robustness provisions relates tu the substituted value. First, is it available, particularly when the source of that value is a real-time input such as a sensor or an operator? Second, does the substitute value allow a resumption of execution without any further downstream processing anomalies under all circumstances?

Another concern is the effectiveness of the fault detection provisions. These provisions, typically assertions in the code, must work for all the anticipated condicions and must not spuriously trigger the substitution when it is not called for. Because robustness can be relied on only for anticipated fault conditions, additional system-level analyses such as Failure Modes and Effects Analyses (FMEAs) and fault tree analyses should be conducted to ensure that major problems have not been overlooked.

The verification issues also apply to rollback. An additional concern is the reliability of the recovery cache and ensuring that data are not corrupted. The recovery cache mechanism typically involves portions of the operating system, memory management scheme (that may include hardware as well as software), and application software procedures that access the cache.

For code to be robust, the substitute value must be available within the time frame required. If this value is contained in the processor memory, then it will be available as required. However, if input from a sensor, operator, or external computer is required, then this input must occur within the required time frame, or a secondary source for substitute values must exist.

For rollback and retry, the recovery action is to restart the calculation. If the calculation is time-critical, this strategy can be problematic. In considering the use of rollback and retry, the designer and verifier must be aware of performance and response time requirements. Reasonable assurance is needed that these requirements can be met even if several retries are necessary before a result is produced. In some cases, an upper limit on the number of retries may be necessary, and a default or other value used when this upper limit is reached. A secondary concern is that nested rollback and retry provisions may cause a propagation of retries (Hitt and Prater, 1987) which could in turn result in a major system processing anomaly.

Coverage is the probability that when a fault occurs, it will be detected and recovery from the fault will be successful. Partial fault tolerance provisions provide error detection and recovery capabilities primarily for anticipated faults. An overriding question is the adequacy of fault detection mechanisms and recovery provisions. In the case of a sensor-reading, conversion, and display task which may be repeating several times per second, the argument for adequacy is fairly clear; even if the provisions fail, new data and a new display will be generated immediately. However, in other cases, e.g., in the scheduling or dispatching portions of an operating system, they may not be.

# 3. N-VERSION SOFTWARE

N-version software, also referred to as multiversion software, relies on voting as the fault tolerance mechanism. Section 3.1 describes the technique. Section 3.2 lists issues of concern to those involved with the validation and certification of this software in flight critical systems.

## 3.1. Description

N-version software uses several independently coded versions of a specified function running in parallel (at least conceptually) (Avizienis and Kelly, 1984). Their output is voted upon, and the majority answer is used as the result. The hardware analogy is passive redundancy, i.e., having n components in parallel with a voter circuit that processes all outputs. The basic strength of the approach is that the code need not be absolutely correct. If enough versions of a critical function have been written, high reliability can be achieved through logical redundancy just as hardware reliability is achieved with physical redundancy.

Figure 3.1-1 shows how a quadruple-version program might be implemented for a quadruple (hardware) redundant flight control system based on work done at Lockheed Georgia (Mulcare and Barton, 1987). Each task would run on a different processor. Input data are placed in one or more buffers. (There may be a single buffer if the four processors can access a global memory). The operating system initiates the execution of the four tasks. As the results are completed, they are passed onto the voting task which assembles the output and determines the majority value. In the quad-redundant configuration shown here, the voter must also have an algorithm for breaking 2-2 ties. For diagnostic purposes the voting task also tracks any disagreements; if a consistent pattern emerges, it notifies the operating system. The operating system then takes an appropriate action, e.g., performing diagnostics and configuring out a processor if versions running on the processor are consistently outvoted. In flight control, where mission lengths typically do not exceed more than 20 hours, a more prudent approach may be to simply retire the processor.

There have been many research projects on N-version programming in addition to the work cited above (Avizienis and Kelly, 1984, and Knight and Leveson, 1986). Two-version programs with a comparator rather than a voter have been certified for flight control and are being used on passenger aircraft. The Airbus A310 slat and flap control systems (Martin, 1982, and Hills, 1985), the Boeing 737-300, 757, and 767 (Yount, 1984), and the Airbus A320 flight control system are all operational examples of 2-version software. For these applications, the primary benefits have been as follows (Yount, 1984):

- More efficient testing: A side-by-side comparison of the two versions aids in the identification of anomalous result.

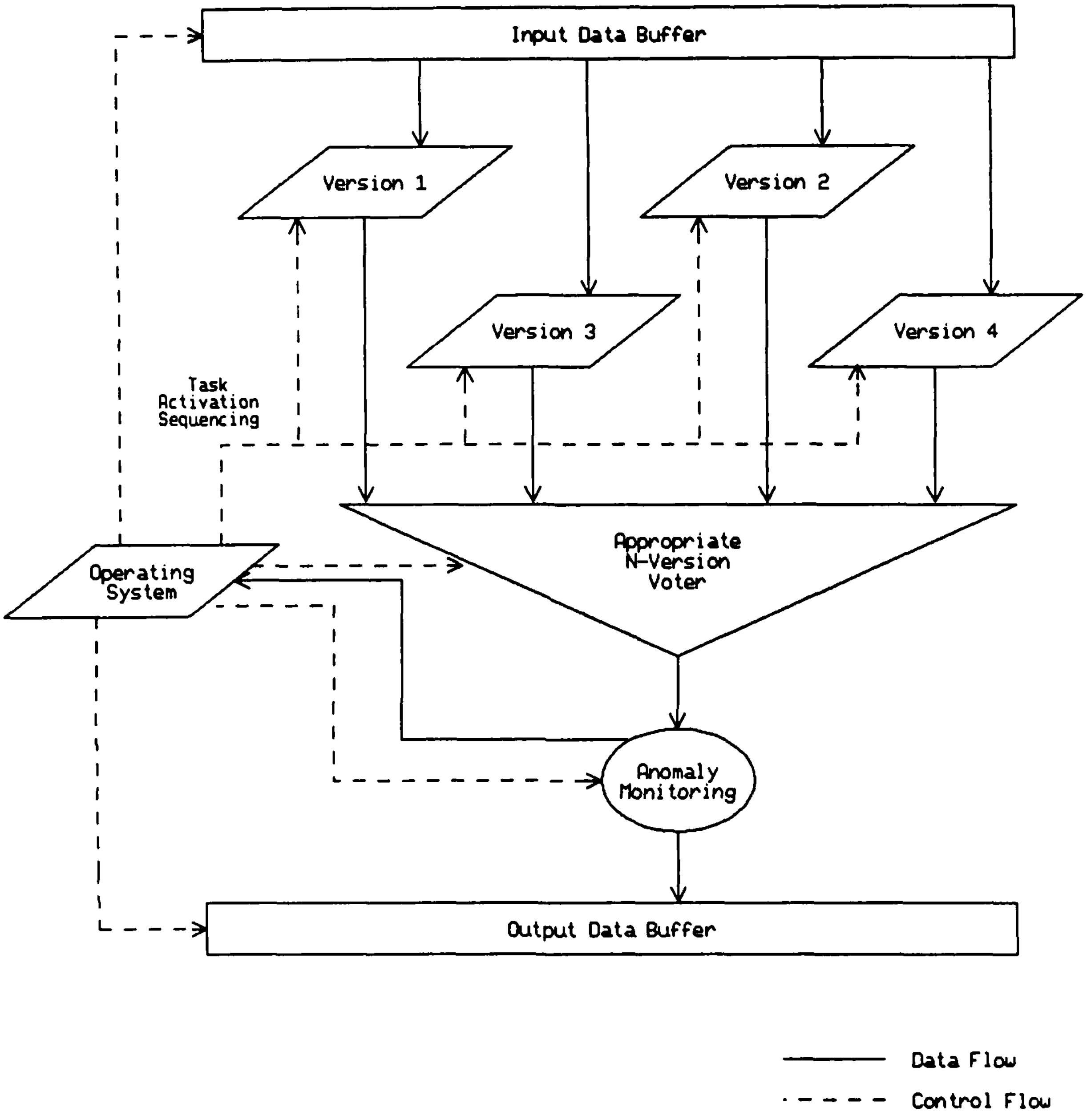


FIGURE 3.1-1. A 4-VERSION SOFTWARE IMPLEMENTATION FOR FLIGHT CONTROL

- Easier certification: The FAA gave tangible credit to Boeing for the use of diverse software.

- Acceptable system reliabilities: With data gathered from 15 airlines, the design Mean Time Between Failures (MTBF) of more than 10,000 hours for the slat and flap control systems was exceeded by approximately 30 percent.

N-version software is a fully fault tolerant technique that provides forward recovery. If a minority of versions are faulty, then the voting process causes their outputs to be disregarded, i.e., masked, and execution proceeds without any delay. This behavior is in contrast to rollback and retry which was discussed earlier or the recovery block which will be described next.

### 3.2. Concerns

Certification of N-version programs for flight critical systems entails a number of significant issues, including software specification, independence of coding faults, the execution environment, recovery of failed versions, and maintenance of multiple versions.

#### 3.2.1. The Software Specification

In conventional software development environments, many misunderstandings that a programmer may have about the application are cleared up in the course of interaction with other members of the development team. However, because the normative N-version programming framework calls for totally separate development efforts, this important but informal supplement to the normal documentation is lost. Therefore, the software specification in N-version programming is of critical importance. A flawed specification will lead to an unreliable program. Therefore, the specification must be complete, consistent, and correct.

Avizienis and Kelly (1984) suggested that a formal specification language be used. Although such a language can reduce ambiguity, it is more difficult for end-users and system-level developers to verify that the specification is a complete and correct statement of what was wanted. Many specification languages are as complicated--or even more complicated--than programming languages. Hence, even if the specifications are complete and correct, they may not be understood by all development team members and outside specialists unless they have specific training in the particular specification language being used.

#### 3.2.2. Independence of Coding Faults

The fundamental assumption of N-version programming is that coding defects are random and uncorrelated. If this assumption is correct, the likelihood of the same fault existing in all or most modules is very low. Unfortunately, this assumption has not been established by experience. A major problem is that a difficult requirement will result in a greater likelihood that all programmers will make the same type of mistake even if the developments are totally isolated from each other. These mistakes, which have been termed correlated errors or faults, are often subtle and difficult to find.

One example of the correlated fault is a proposed recent airworthiness directive issued by the FAA for the 737-300 flight control system noted earlier. There have been reports of at least 18 uncommanded flight control changes. These uncommanded changes apparently occur once every several thousand times that an aircrew resets the target altitude in the autopilot's altitude select window (Aviation Week, 1988). A second example of a correlated error was that the hardware implementations of floating point arithmetic on the VAX 11/780 computer did not allow for adequate precision for some cases in an experiment performed at the University of Virginia and the University of California, Irvine, in 1985 (Knight and Leveson, 1986).

The problem of independence among versions is compounded by the fact that all versions must produce output in exactly the same format, at the same rate, and with the same precision in order for the voting algorithm to be kept simple and reliable.

One way to relieve some of these drawbacks is the notion of directed N-version design. Instead of relying totally on independence to produce the required degree of diversity, specifications for the different versions could be written to include some algorithmic constraints. These constraints might include the order of operations, specific numerical techniques that may or may not be used, or specified differences in techniques, e.g., table look-up versus direct calculation.

### 3.2.3. Run-time Environment

As figure 3.1-1 shows, N-version programming involves more than the n programs and a voter. The run-time environment for execution of this software in a flight control system must include provisions for:

- Inputting identical data to all versions.

- Synchronizing all versions; i.e., in order to perform a valid vote, each version of the software must complete within a certain time interval, and all results must be from the current execution frame or time slice.

- Collecting results for input to the voter.

- Routing the results of the voter to the appropriate destination, e.g., an actuator motor or display.

- Data recording and diagnostics so that consistently disagreeing versions--and possibly their associated processors if they run in a multiprocessing environment--are configured out of the operational system for the duration of the mission.

The run-time environment is critical to the correct functioning of the technique and must be protected. If the software and hardware components of the environment are incorrectly designed or become corrupted during a flight an unrecoverable system failure will probably occur.

### 3.2.4. Recovery of Failed Versions

If the application requires awareness of past events; e.g., for integration or averaging, filtering, or target tracking, a failed version must have its data structures updated before participating in subsequent votes. The nature of the updating mechanism, techniques for performing the update, and synchronization techniques are application dependent. However, their correctness is critical for realizing the potential reliability benefits through restoration of a failed resource.

### 3.2.5. Maintenance and Upgrades

Questions of maintenance affect errors in a single version and across all versions. In a single version, there is a question of whether a known bug should be altered if it has not been found in other versions. Economic considerations, configuration management problems, and the concern that fixing a known bug can introduce additional unknown problems must all be addressed before a decision is made.

Management of a version-wide modification presents other problems. If the same maintenance coder modifies all versions of the software, independence is lost. On the other hand, it is impractical to have four or five different coders maintaining different versions. The practices of the developer in handling this problem can have a significant impact on the reliability of the software once the development is concluded.

# 4. *RECOVERY BLOCKS*

Recovery blocks are a backward recovery technique which incorporate explicit error detection and recovery provisions. In this regard, they are related to the rollback technique described in section 2. However, they include redundant logic in the form of an alternate routine which is used if an error is detected. They are therefore fully fault tolerant. Section 4.1 describes the basic recovery block and its variations. Section 4.2 lists concerns related to their validation in flight-critical software.

## 4.1. Description

Recovery blocks were first described by B. Randell of the University of Newcastle in 1975 (Randell, 1975). The three elements of the basic recovery block are:

- The primary routine which implements a given function or program specification.
- The acceptance test which determines that the requirements of the function or specification have been met after each execution of the primary routine.
- One or more alternate routines which perform the same function as the primary routine using an independent algorithm. The alternate routines are invoked if the acceptance test condition is not met.

The basic structure of a recovery block with only a single alternate routine is shown in figure 4.1-1. Randell stated it formally as:

```
Ensure AT

          By P
          Else by Q

Else Abort
```

Where AT is the acceptance test, P is the primary routine for a given function, Q is the alternate, and the Abort condition invokes a higher level recovery procedure. When more than one alternate is provided, additional 'Else by...' statements (i.e., Else by R, Else by S, etc.) follow 'Else by Q'. Until the acceptance test is passed, the input data are protected in their original state by a recovery cache in a manner similar to the fault containment structure described in section 2.

Important features of the recovery block are:

- Software outside the recovery block is unaffected by which routine (primary or alternate) furnished the satisfactory result.

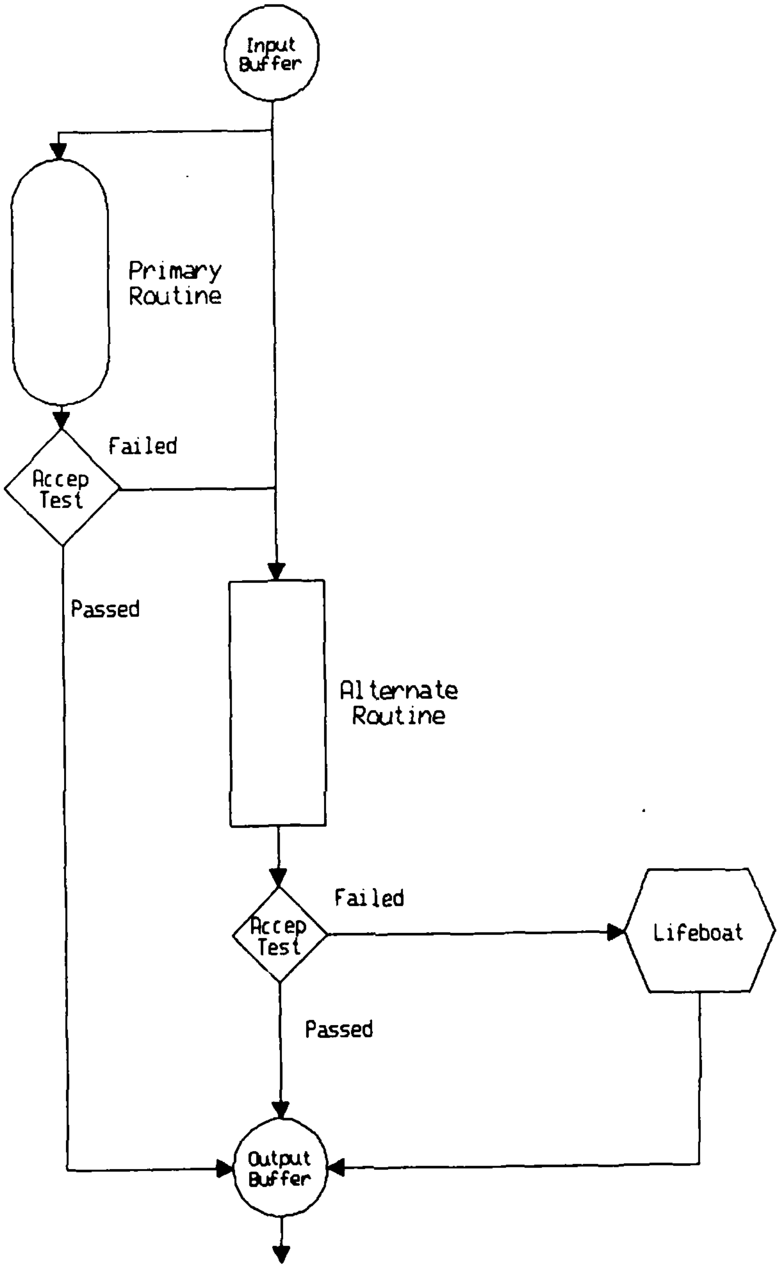


FIGURE 4.1-1. BASIC RECOVERY BLOCK

- The alternate routine is executed only upon a failure of the primary routine. Thus, the alternate can use inefficient but highly failure-resistant code; this avoids a run-time penalty under normal conditions.

- The recovery block allows for a subsequent retry of the primary routine. Software failures result from the inability of the program to process a specific set of input data when in a certain computer state. Therefore, it is undesirable to make a permanent switch to the backup module after only an isolated failure in the primary routine. Returning to the primary may be desirable because of greater efficiency, versatility, or confidence. A simple diagnostic procedure can be used to switch the roles of the primary and backup modules when repeated failures of the primary occur.

- Failures of individual routines are visible from the state of a flag set by the acceptance test AT. Therefore, online monitoring and testability are readily incorporated into the recovery block. The technique also permits capture of the data associated with each failure. Hence, complete diagnostic information for later improvements of software can be made available.

In order to implement recovery blocks effectively, the primary routine, alternate routine, and acceptance test must be deliberately independent. This approach contrasts with N-version programs where independence is usually assumed to be implicit by virtue of the independent development of the versions. Deliberate independence can be achieved in a variety of ways. In mathematical and logical operations, the basic commutative, associative, and distributive properties can be used to change the order of calculation. In systems which control physical processes, it may be possible to derive a result from several different physical inputs.

In a demonstration of recovery blocks for use in flight navigation (Hitt and Prater, 1987), independence was achieved by removing some of the functionality in the primary routine. However, because no alternative to the fundamental form of the navigation equations was available, an approximation of the sine and cosine functions was used in the alternate version; the primary relied on library trigonometric routines in the Ada compiler that was being used.

Acceptance tests can often be designed to check for a plausible result rather than a correct result. For example, data processed from sensors and sent out to actuators can be checked for continuity; i.e., the difference between the value of a previous iteration and the current value should be less than some stated limit.

An additional consideration for real-time applications is to ensure that computations are completed in the required time. One possible approach is the inclusion of a "watchdog timer" which forces entry into a recovery condition if the acceptance criteria are not met within a given time. The structure of such a recovery block is shown in figure 4.1-2.

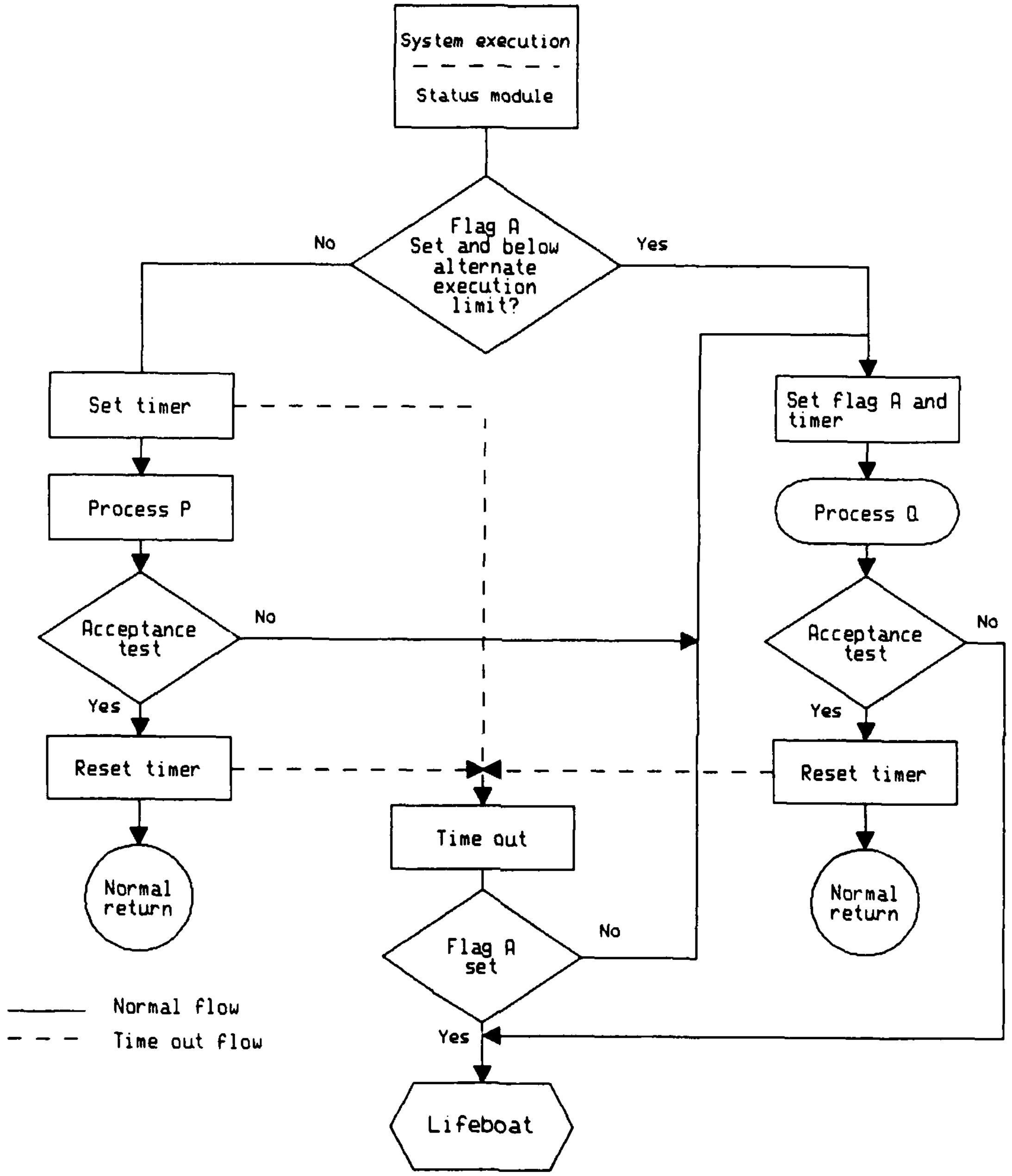


FIGURE 4.1-2. RECOVERY BLOCK FOR REAL-TIME APPLICATIONS WITH A SINGLE WATCHDOG TIMER

Before entering the recovery block, calls to the primary and alternate routines are prepared, and the allocated execution time (including an allowance for the acceptance test) is loaded into the watchdog timer. The primary call is then executed and the result of the processing is subjected to the acceptance test. If passed, a normal return results. If not passed or if the watchdog timer interrupts the primary process, the alternate routine is executed and the acceptance test is run on its results. Once again, a normal return will take place if the results pass the acceptance test. However, if the alternate routine also does not produce an acceptable result or if an alternate routine time-out occurs, then an abort-return results and recovery must take place on a higher level.

Figure 4.1-3 (Hitt and Prater, 1987) shows the flow chart for a recovery block implemented with two watchdog timers: The first is for the "minor frame," i.e., the time allotted for execution of the total recovery block. The second is for each version of the software. The function of this second watchdog timer is similar to the single watchdog timer example described in the previous paragraph.

An additional variation on recovery blocks is nesting. In a nested recovery block, a failure of the lower level primary and alternate would cause a return to the higher level recovery block with a failure indication. The higher level recovery block would then invoke its alternate higher level routine. The advantage of such a structure is that it provides additional software redundancy, and that a single higher level alternate routine may substitute for a number of secondary or tertiary alternates on a lower level. The primary cost is a performance penalty because rollback to an earlier stage in execution must occur to effect a recovery.

When both the primary and alternate routines are implemented on a single processor, the performance penalty entailed by rolling back and restarting the calculation with an alternate routine using data in the recovery cache may be unacceptable. However, because most future digital flight control designs will have several processors, it is possible to use a Distributed Recovery Block (DRB) (Kim 1984) as shown in figure 4.1-4. In the DRB, each processor contains its own copy of the primary and alternate. The processor in control of the system executes the primary routine and the backup processor(s) execute(s) the alternate routine(s) in parallel. All processors run the same acceptance test. Thus, if the primary processor fails, the backup processor's results are already available with no time lost for the retry. The use of different processors with different versions of the software unifies both hardware and software fault tolerance into a single framework of distributed systems fault tolerance. This integration provides protection against a broader scope of problems (i.e., both hardware and software failures) and has significant performance advantages. Additional research should be pursued on issues such as identifying the actions to be taken following a failure and integrating hardware status checks into the DRB (Hecht, 1988).

There is little data available on the effectiveness of recovery blocks in operational systems. However, early results indicate that increases in software MTBF on the order of two to three times could be achieved in an academic setting (Anderson, et al., 1985). The authors suggest that significantly higher

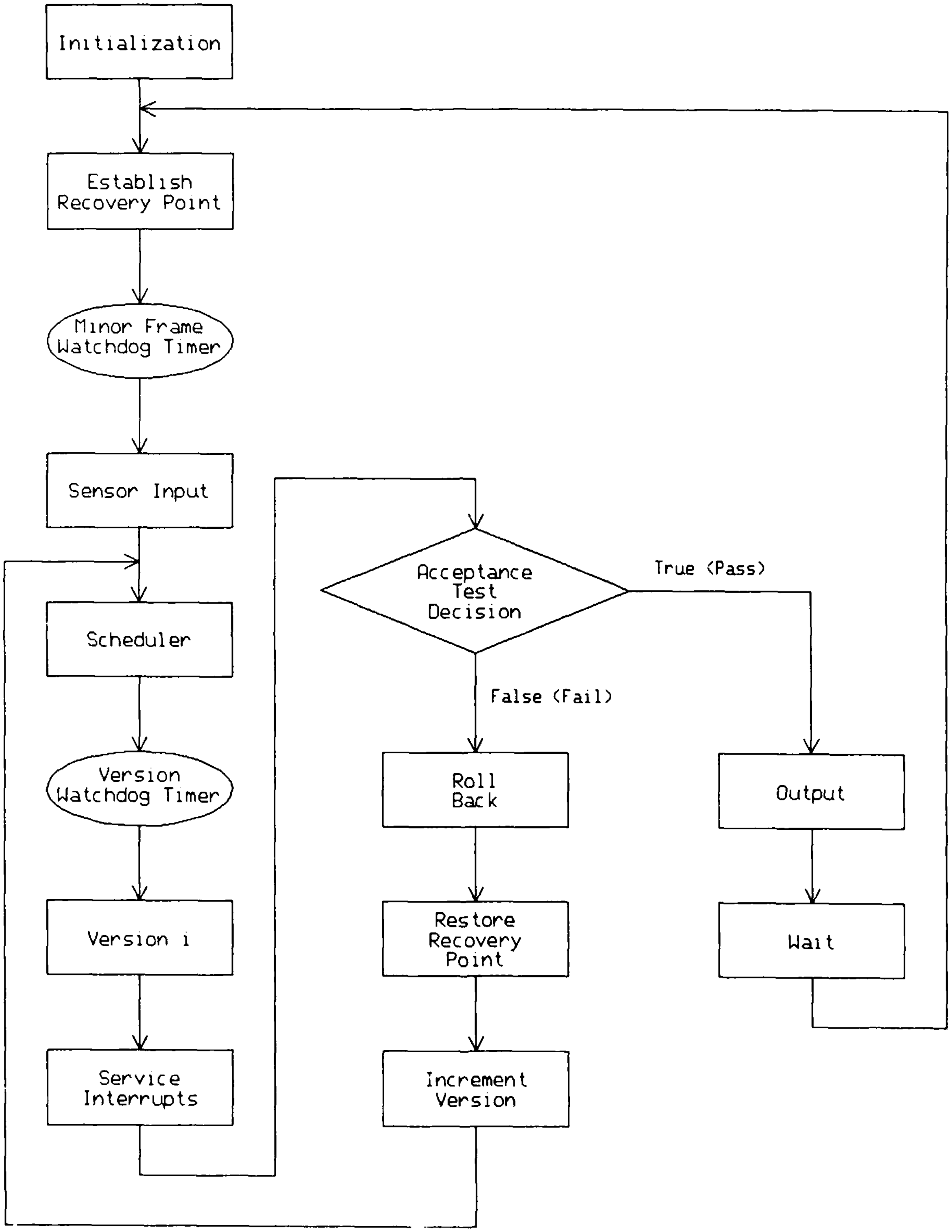


FIGURE 4.1-3. A REAL-TIME RECOVERY BLOCK WITH TWO WATCHDOG TIMERS

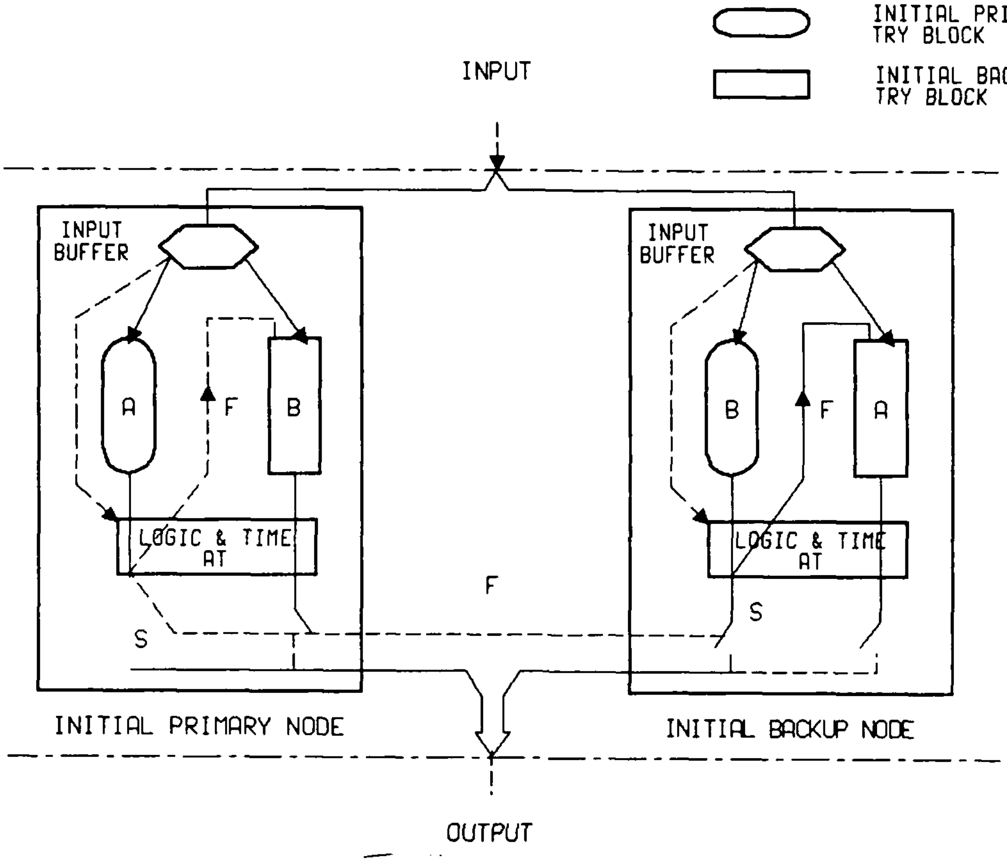


FIGURE 4.1-4. DISTRIBUTED RECOVERY BLOCK

reliability increases can be expected in a conventional software production setting; system-unique factors were cited as underestimating the true effects of software fault tolerance in this particular experiment.

## 4.2. Critical Issues

Critical issues for recovery blocks used in flight critical software include the correctness of the acceptance test, reliability of the underlying operating environment, and independence of the alternate routine.

### 4.2.1. Acceptance Tests

The acceptance test is a single point of failure in the recovery block. The two possible failures are: First, that the acceptance test accepts an incorrect result. Second, that the acceptance test rejects a correct result. The consequences of both failures can be serious. For example, failure to detect erroneous navigation data may result in an aircraft flying into the flight path of another aircraft, an unauthorized airspace, or a military conflict area. The acceptance test's spurious rejection of correct results by both the primary and the alternate routine will result in a cessation of computation and a total failure of the recovery block.

The most effective means of minimizing this risk is fault avoidance in the acceptance test. Specifically, the acceptance tests should be very simple and amenable to thorough verification. The need to create simple, verifiable acceptance tests should be considered when designing the construction and modularization of this system. Further considerations in the use of fault avoidance versus fault tolerance are listed in section 5.

A second method of reducing the risk of defective acceptance tests is through nesting. Mitigation of the non-detection risk occurs because a faulty result may cause an acceptance test failure in subsequent calculations. This, in turn, can cause a rollback to an alternate routine which resumes the calculation using data unaffected by the fault. Mitigation of the spurious rejection risk occurs because the alternate path will use a different set of acceptance tests than was used on the primary path. However, there is a significant performance penalty in nesting. Extensive rollback can cause response time requirements to be missed. This performance penalty may not be acceptable in unstable aircraft because an unrecoverable situation can occur if the control system does not react in time.

### 4.2.2. Run-time Environment

As is the case for all other software fault tolerance techniques, there is a dependence on the underlying operating system and run-time provisions. Concerns for recovery blocks are: maintenance of the Recovery Cache, invocation of the Alternate Routine, and maintenance of the Watchdog Timer.

Where the mechanisms for these functions are sufficiently simple, they can be subject to exhaustive verification and considered to be part of the protected, unalterable, "hard core" of the operating system. In other cases, these mechanisms can in and of themselves be made fault tolerant and rely on simpler mechanisms contained within an operating system hard core.

### 4.2.3. Independence of the Alternate Routine

The type of degree of independence required in the alternate routine is determined largely by the nature of the fault classes which are anticipated. In the recovery block implementation for the navigation system cited above, independence was achieved by avoiding use of library procedures in the alternate routine. This measure ensures that precision or other subtle problems in the libraries will not affect the result. Because the alternate used the same equations as the primary, however, the developers needed to ensure that these equations would not be a source of error.

In other cases, it may be acceptable to use the same underlying library routines in both versions while using different equations or algorithms. This measure is appropriate if the developers are concerned about the appropriateness of the algorithms. A third measure is to use different languages and different libraries for the primary and alternate. The availability of a reliable linking and calling mechanism alleviates the concerns of defects in libraries and compilers.

Definition of the degree of independence should be based on system-level reliability analyses performed as a part of the design process. During the validation of flight control systems, the analyses, the independence requirements derived from these analyses, and conformance with these requirements must be performed.

## 5. FAULT AVOIDANCE VERSUS FAULT TOLERANCE

Fault tolerant software provisions have costs in terms of development time, processing overhead, and recovery time. In addition, these provisions rely on underlying systems software or firmware in order to function properly. Thus, fault tolerance is not a substitute for fault avoidance, i.e., traditional software development practices designed to eliminate coding defects. These practices include:

- Software Development Process Controls including formal requirements generation, design methodologies, structured programming reviews, inspections, and configuration management.

- Software Testing at the unit, Computer Software Component (CSC), and Computer Software Configuration Item (CSCI) level.

- IV&V of deliverables, procedures, practices, and standards.

Ideally, stringent controls during the software development process can ensure that the entire project team works from a single design, uses well-defined interfaces, follows consistent variable naming and typing conventions, and develops adequate documentation. However, while such control can prevent faults due to a lack of communication or coordination among various team members, it cannot guarantee that subtle (or not so subtle) flaws in the specification or detail design will not result in faulty code. These design flaws are most likely to occur when timing, synchronization, exception handling, input/output, or interprocessor communication are involved.

Software testing can occur at the unit, component, and configuration item level. Strategies used in testing include branch testing, path testing, testing for singularities of critical variables, independent testing, and use of automated test tools. An important test methodology that has not received much attention in the literature is stress testing, which is deliberately exposing the program to faulty data sets or higher workloads than called for in the specification. Although still subject to the general limitations of testing, stress tests will frequently expose performance deficiencies which are not addressed by other strategies.

Code verification compares the detailed design with the actual code and devises tests and inspections that indicate compliance. Validation is done over a larger scope of system development, e.g., comparison of the delivered code with the A-specification or a lower level requirements document. For large real-time systems in critical applications, it is current practice to have a separate organization perform the IV&V. Usually, such IV&V activities are performed using standard procedures and sampling methods that are intended to provide a reasonable but by no means complete demonstration that the code fulfills its requirements.

Examples of where fault avoidance measures are either necessary or more efficient than real-time fault tolerance provisions include:

- Critical operating system software: Software that manages the invocation of fault-tolerant tasks; i.e, queues, buffers, interrupts, and timers must function flawlessly in order for the fault tolerance provisions to work effectively. Modules which perform these functions are generally large and may be amenable to the inclusion of fault tolerance provisions. However, there is still the need for total verification of these fault detection, isolation, and recovery provisions. Normal verification techniques described above are unsuitable for these critical code sections. More intensive techniques such as the Enhanced Condition Table (Tai, Hecht, and Hecht, 1987) together with extensive testing on the target system are generally needed.

- Constants: Faults in constants embedded in the code (e.g., size of memory or number of mailboxes for interprocessor communication) cannot easily be detected by fault tolerance provisions but can be readily found during pre-operational verification activities. System-level reliability analyses such as FMEAs and fault-tree analyses can be used to identify critical constants which must be verified. Utility programs or test tools can be built to perform this verification automatically or semi-automatically.

- Simple sections of code: While verification of entire real-time software systems is impractical, it may be possible to totally verify certain small sections of code--particularly if their input domains and operational environments are well-defined, and there are no timing or communication dependencies. Even when fault tolerance provisions can be defined, run time penalties and the need for additional exception handling frequently make them less desirable alternatives to fault avoidance.

- Static data: Many initiating events in software failures are related to input data. While much of the data in a flight control system is dynamic, there are significant portions which are static, e.g., geographical positions and aircraft parameters. As was the case for constants embedded in the code, verification and automated tools can be an effective and efficient means of detecting and correcting faults in such data.

On the other hand, fault avoidance provisions cannot be relied upon to provide complete coverage when the state of the system cannot be determined in advance. Examples include:

- Interprocessor communication: Requirements for interprocessor timing, sequencing, and message processing (whether on the same bus or from another network node) are generally not totally predictable during the design phase. Thus, it is generally impossible to develop a complete set of test cases that demonstrate correct functioning of the communication and message processing software. Under these circumstances, fault containment is a better approach. Data from interprocessor communication can be checked for integrity using error coding techniques, for reasonableness using range checking or wraparound tests, and for security using various encoding schemes. Failure to pass these tests can cause a retry, substitution of default values, or use of previous values.

- Input/output: As was the case previously, the timing, content, and format of incoming messages cannot be predicted with sufficient certainty that an exhaustive set of test vectors can be produced. Under such conditions, online assertion checking such as that contained in fault containment or recovery blocks will constitute a more reliable approach.

- Critical response times: When it is difficult or impossible to ensure that all response time requirements will be met, a recovery block (which includes a watchdog timer as part of the acceptance test) is generally necessary.

# 6. INTEGRATION OF FAULT TOLERANCE TECHNIQUES

The previous sections have described critical issues and limitations associated with specific techniques. However, many of these limitations can be overcome by judicious combination of different fault tolerance techniques and the use of fault avoidance. Table 6-1 lists considerations that affect the choice of methods. The following subsections discuss the specific considerations in greater detail.

## 6.1. Coverage

Most robustness provisions address specific fault types, such as data out of range or improper arguments passed to a program. Fault containment and recovery blocks can use reasonableness or other types of acceptance tests which provide much broader scope and do not require prior knowledge of the expected faults. N-version programming provides the broadest coverage because its only limits are the common assumptions used in the specification or the design of all versions.

## 6.2. Retry Requirements

Retry of the same program always entails a possibility that the failure will be repeated in subsequent trials. Retry also impacts timing and throughput requirements. As long as no errors are encountered, the additional execution time is expected to be small; it is limited only to the assertion check at the end of the routine. However, when errors are encountered, the execution time may increase considerably--perhaps beyond the acceptable limits for time-critical applications. Because of the rarity of exception cases, average execution time is hardly affected by this consideration.

Failures covered by rollback can be resolved by assignment of default values or similar forms of forward recovery. Thus, retry is not always necessary using fault containment or robustness techniques.

By way of contrast, recovery blocks always use a new program if there is a failure. Similarly, use of N-version code does not require a retry because the final output is determined by a majority vote. Thus, for critical timing requirements or where fully fault tolerant software is necessary, the preferred techniques are N-version software or recovery blocks.

## 6.3. Cost and Complexity

Cost factors are related to the introduction of additional code including the development and maintenance expense of additional code and resources utilized during execution. Additional code introduces complexity which in turn increases the likelihood of added faults. Because robustness and rollback require relatively little additional code, fault tolerant development costs represent only a minor fraction of the total cost for the delivered code. So long as retry is acceptable, these two techniques also impose the lowest overhead.

TABLE 6-1. SOME RELEVANT CHARACTERISTICS OF FAULT TOLERANCE TECHNIQUES

| Techniques | Coverage | Retry[1] | Cost and Complexity |
|---|---|---|---|
| Robustness | Narrow (specific to anticipated faults) | No (default or alternate is used) | Generally low |
| Rollback | Can be broad (determined by assertion) | Usually (default may be used) | Low to medium |
| Recovery Block | Broad (determined by acceptance test) | No (handled in alternate routine) | High |
| N-version software | Very broad (limited only by assumptions in the specifications common design assumptions | No (N-version run once) | High to very high |

[1] Whether a retry of the same code which induced the fault initially is necessary.

When the recovery block is used, at least three independent sections of code (the primary routine, the alternate routine, and the acceptance test) have to be designed, coded, tested, and maintained. A considerable increase in cost and complexity is therefore incurred. In most cases, the acceptance test is small relative to the code being tested and hence, run-time overhead is low. However, the alternate routine may be significantly less efficient than the primary routine when an error condition occurs, and repeated execution of the entire recovery block (i.e., primary, acceptance test, and alternate routine) may result in a major throughput penalty. The likelihood of such an occurrence should be assessed as part of the design process.

In N-version software cost can be even higher because (1) multiple versions must be developed separately and (2) special development of specifications may be necessary to ensure that programmers can work independently and produce compatible results. During run-time, throughput is limited to the slowest of the routines. If the technique is practiced using true independence, it may not be possible to know the extent of this run time penalty until after completion of the coding when it may be too late. This run-time risk must be assessed as part of the software design because it may ultimately be the major cost driver in the development.

A major cost common to all fault tolerant techniques is verification during both development and maintenance. The verification of recovery provisions is generally difficult, and the major function of fault tolerance is to provide for recovery. For fault containment and recovery blocks, the goal of verification is to ensure that the acceptance test correctly identifies all error conditions and does not spuriously identify an acceptable result as a failure. For N-version programming, verification must be performed on all versions of the routine as well as on the voter for all possible results. During maintenance, thorough testing is necessary in order to ensure that coding changes do not defeat fault tolerance measures that are already in place.

Because of the high cost associated with fault tolerant software development, maintenance, and verification, its use should be restricted to functions critical to the continued safe operation of the system.

## 7. CONCLUSION

In order to achieve the very high reliability required in flight-critical systems, traditional software development methods are insufficient. Fault tolerance provisions can provide the additional reliability by detecting and recovering from faults occurring within the software before they affect aircraft operation and safety. However, in order to be effective, decisions on which fault tolerant techniques to use, where they are to be applied, and how they are to be verified must be made early in the design process and in the framework of the appropriate system-level analyses such as FMEA and Fault Tree Analysis.

The proper choice of fault avoidance versus fault tolerance, and judicious application of the appropriate fault tolerance techniques will result in a maintainable, cost effective, reliable, and high performance system. Those involved in the validation and certification of flight-critical digital systems should ensure that these analyses have been performed, and that they take into account the strengths and weaknesses of the techniques that have been described in this chapter.

# BIBLIOGRAPHY

Anderson, T., et al., Software Fault Tolerance; An Evaluation, University of Newcastle upon Tyne, Technical Report No. 202, September, 1985.

Avizienis, A. and J. P. J. Kelly, "Fault Tolerance by Design Diversity: Concepts and Experiments," Computer, Vol. 17, No. 8, pp. 67-80, August 1984.

Chen, L. and A. Avizienis, "N-Version Programming: A Fault Tolerance Approach to Reliability of Software Operation," Digest of Papers, FTCS 8, pp 3-9, June 1978.

Data and Analysis Center for Software (DACS), "Quantitative Software Models," DACS SRR-1, March 1979.

Davis, E. A. and P. K. Giloth, "No. 4 ESS: Performance Objectives and Service Experience," Bell System Technical Journal, Vol. 60, No. 6, pp. 1203-1224, August, 1981.

Dijkstra, E. W., "Notes on Structured Programming," Structured Programming, Academic Press, New York, 1972.

Harvey, P. R., Fault Tree Analysis of Software, Thesis for the Master of Science in Information and Computer Science, University of California at Irvine, 1982.

Hecht, H. and M. Hecht, "Use of Fault Trees in the Design of Recovery Blocks," Proceedings 1982 Fault Tolerant Computing Symposium (FTCS-12), Santa Monica, CA, June, 1982.

Hecht, H. and M. Hecht, "Fault Tolerant Software," Fault Tolerant Computing, D. K. Pradhan, ed., Prentice Hall, Englewood Cliffs, NJ, 1986.

Hecht, M., "Extended Distributed Recovery Blocks," Proceedings of the Annual National Joint Conference on Software Quality and Reliability, National Security Industrial Association, Arlington, VA, March, 1988.

Hills, A. D., "Digital Fly-by-Wire Experience," Proceedings AGARD Lecture Series No. 143, October, 1985

Hitt, E. F. and S. A. Prater, Navigation Recovery Block Design Description, Federal Aviation Administration Technical Center, DOT/FAA/CT-87-15, Atlantic City, 1987.

Howden, W. E., "An Evaluation of the Effectiveness of Symbolic Testing," Software-Practice and Experience, Vol. 8, pp. 381-397, John Wiley & Sons, 1978.

Kelley, J. P. J., "A Specification Oriented Multi-Version Software Experiment," Proceedings of the 13th International Conference on Fault Tolerant Computing (FTCS-13), Milan, Italy, 1983.

Kim, K. H., "Distributed Execution of Recovery Blocks: An Approach to Uniform Treatment of Hardware and Software Faults," Proceedings of the 4th Annual International Conference on Distributed Computing Systems, pp. 526-532, IEEE Cat. No. 84CH2149-3, May, 1984.

Knight, J. and N. Leveson, "An Experimental Evaluation of the Assumption of Independence in Multiversion Programming," IEEE Transactions Software Engineering, Vol. SE-12, No. 1, pp. 96-109, January, 1986.

Martin, D. J., "Dissimilar Software in High Integrity Applications in Flight Control," Proceedings AGARD CPP-330, September, 1982.

Miller, E. F., Jr. et al., "Application of Structural Quality Standards to Software," Software Eng. Stand. Appl. Workshop, IEEE Cat. 81CH1663-7, pp. 51-57, July 1981.

Mulcare, D. B. and L. A. Barton, N-Version Software Demonstration for Digital Flight Controls, Federal Aviation Administration Technical Center, *DOT/FAA/CT-86/33*, April, 1987.

Randell, B., "System Structure for Software Fault Tolerance," IEEE Transactions on Software Engineering, Vol. SE-1, No. 2, pp. 220-232, June 1975.

Tai, A., M. Hecht, and H. Hecht, "Enhanced Condition Table Method for Verification of Critical Software," Proceedings of the 11th Annual International Computer Software and Applications Conference (COMPSAC87), IEEE Computer Society Press, pp. 317-323, October, 1987.

Yau, S. S. and R. C. Cheung, "Design of Self-Checking Software," Proceedings 1975 International Conference on Reliable Software, IEEE Cat. 75CH0940-7CSR, pp. 450-475, April 1975.

Yount, L. J., "Architectural Solutions to Safety Problems of Digital Flight Critical Systems for Commercial Transports," Proceedings AIAA/IEEE Digital Avionics Systems Conference, Long Beach, CA, December 1984.

## GLOSSARY

A-SPECIFICATION. The highest level specification typically produced by the contracting organization to define a system (see MIL-STD-1521).

BACKWARD RECOVERY. Restoration of the system to some previous known correct state and restarting the computation from that point.

COVERAGE. The probability that when a fault occurs, it will be detected and recovery from the fault will be successful.

FAULT AVOIDANCE. The attempt to prevent any software faults in the final delivered product through disciplined software development practices, testing, and IV&V.

FAULT CONTAINMENT. The capacity of a system to prohibit errors and/or failures from propagating from the source throughout the system.

FAULT TOLERANCE. The capability to endure errors and/or failures without causing total system failure.

FAULT TOLERANCE. Software which continues to operate satisfactorily in the presence of faults.

FORWARD RECOVERY. Restoration of the system to a consistent state by compensating for inconsistencies found in the current state so that the system may continue processing.

GLASS COCKPIT. Advanced state-of-the-art electronic displays utilizing flat panel and/or cathode ray tube display technology for cockpit instrumentation.

RECOVERY CACHE. The location used to preserve input values until the outputs resulting from them have been accepted.

ROBUSTNESS. The ability of the code to perform despite some violation of the assumptions in its specifications usually via substitution of an alternate value and continuation of execution if a software fault is detected.

ROLLBACK. Retrying the calculation in the event that a failure is detected, under the assumption that some external condition may have changed thereby resolving the anomaly.

# ACRONYMS AND ABBREVIATIONS

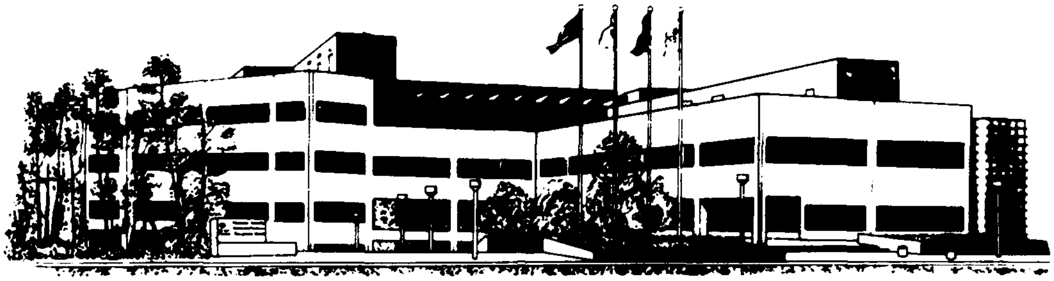
| | |
|---|---|
| AIAA | American Institute for Aeronautics and Astronautics |
| CSC | Computer Software Component |
| CSCI | Computer Software Configuration Item |
| DRB | Distributed Recovery Block |
| ESS | Electronic Switching System |
| FMEAs | Failure Modes and Effects Analyses |
| IEEE | The Institute for Electrical and Electronics Engineers, Incorporated |
| IV&V | Independent Verification and Validation |
| MTBF | Mean Time Between Failures |

S. Department of Transportation
ederal Aviation Administration

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II DIGITAL SYSTEMS VALIDATION

## CHAPTER 10 LATENT FAULTS



PREPARED BY:

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

PREPARED FOR:

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

# 1. INTRODUCTION AND HISTORY

The reliability of a flight control system (FCS) is achieved by a combination of (1) reliable components, (2) redundancy, and (3) the ability of the FCS to detect, isolate, and recover from faults. All highly reliable FCS designs incorporate some form of comparison-monitoring to detect faults. When the fault, or rather, the error produced by the fault, reaches a comparator it is immediately detected, at which time the isolation and recovery mechanisms are invoked.

Experience has shown that comparison-monitoring is an effective and reliable means of detecting faults. Moreover, because a comparator only detects a fault when the fault produces an error, it retains the faulty component for as long as the component functions correctly. In the interim, the fault may remain latent for long periods of time before it finally produces a malfunction. To detect these latent faults, some form of self-test is employed, either in a preflight or maintenance test or, during flight, in background.

With respect to latent faults, the critical issues are:

- What proportion of faults are latent?
- What mechanism activates a latent fault?
- What are the effects, if any, of latent faults on aircraft survivability?
- If latent faults are a contributing factor to reduced survivability, what level of coverage is required to detect and eliminate them?

Prior to the Fault Insertion and Instrumentation System (FIIS) experiments (the results and implications of which comprise the subject matter of this tutorial), most of the published information on data latency in digital FCSs was obtained from two important studies conducted independently by Bendix (McGough and Swern, 1983) and by the Charles Stark Draper Laboratories (CSDL) (Lala and Smith, 1983).

## 1.1. Bendix Study

The purpose of this study was to estimate detection coverage of several candidate self-test programs and to estimate fault latency in a conventional digital FCS. Fault injection experiments were conducted on a software-simulated version of the Bendix BDX-930 bit-sliced flight control computer (FCC), which featured the 2901A arithmetic logic unit (ALU) as the principal processing element. The simulated components consisted of the central processing unit (CPU), micromemory, program memory (ROM), and random access memory (RAM). The input/output (I/O) circuitry was not simulated. Sensor inputs were randomly generated and deposited in RAM at the start of each computational frame. Each device of the CPU was represented by a gate-equivalent circuit and stuck-at faults were injected at the gate nodes, something not possible in actual hardware fault testing. The micromemory was represented functionally and faults were simulated by reversing the logic states of single bits.

The ROM and RAM memories were also represented functionally but no faults were injected into these devices. Faults were randomly selected and injected, one at a time. Fault selection was weighted in proportion to the failure rate of the device (i.e., the average number of faults injected into a particular device was proportional to the device failure rate). The simulation technique was "parallel mode," which allowed for the simultaneous simulation of up to 32 computers, one of which was always the non-failed version. This made it possible to compare the responses of the failed and non-failed computers at any time in the compute cycle and at any device.

Although all devices were simulated at the gate-level, faults were injected at both the pin-level and gate-level in order to determine differences in detection coverage between the two fault types.

Two types of experiments were conducted, depending upon the method of detection:

- To determine the effectiveness of comparison-monitoring, the computed outputs of a failed and non-failed computer were compared at the end of each frame. Any discrepancy was defined as a "detected failure". These comparisons were performed by the simulator executive and did not involve the detection mechanisms that would normally be resident in the FCCs. Each computer executed the same flight control program, which consisted of the inner loops of a high performance aircraft. In order to reduce the simulation time, a fault run was terminated after detection or after eight repetitions, whichever occurred first. To avoid any ambiguity in the comparison process, each computer received identical sensor inputs at the start of each frame. The simulation was conducted "open-loop", with sensor values selected independently and at random.

- To determine the effectiveness of self-test, each fault was injected and a candidate self-test program was executed. A fault was defined as "detected" if the mechanism of the self-test routine so indicated.

## 1.2. Charles Stark Draper Laboratories Study

The purpose of this study was to assess the fault detection, identification, and reconfiguration capabilities of the CSDL-designed fault-tolerant multiprocessor (FTMP). This system featured the Rockwell/Collins CAPS-6 computer as the principal processing element. The CAPS-6 is similar to the BDX-930 in that it, too, is a bit-sliced processor utilizing the 2901A ALU. FTMP is a triple modular redundant (TMR), bit-synchronized multiprocessor, designed for ultra high reliability ($10^{-10}$ failures/hour) and fault-tolerance. The design is based on independent processor-cache memory modules and common memory modules, which communicate via redundant serial buses. All information processing and transmission is performed in triplicate. Data transmitted over the bus network is monitored by Bus Guardian Units (BGUs), which compare the transmitted data, bit by bit. Faults are detected when they produce errors at the BGUs. Faults are also detected by self-test programs, which are executed continuously in background.

The fault injection experiments were conducted on real hardware. Stuck-at faults were injected, one at a time, on device pins of one of the three processing elements. (The fault injection hardware was identical to that used in the FIIS experiments.) Faults were systematically selected (unweighted) and injected on pins of eight circuit boards. FTMP executed a flight control software program consisting of inner-loops and autopilot modes, which were patterned after the L-1011 Tristar FCS. The fault runs were terminated after 15 seconds of real time. Unlike the Bendix experiments, the simulation was closed-loop (i.e., the sensor values were obtained from the motion parameters of a simulated aircraft).

## 1.3. Results

Both studies indicated that most faults are were detected within a few computational frames of their occurrence (e.g., 0 to 500 ms). Because fault runs were terminated after eight repetitions, the Bendix study gave no information about detection beyond 800 ms (assuming 100 ms per frame). The CSDL results indicated that relatively few faults (2 to 4 percent) were detected in later repetitions and these were detected by background self-test programs. From these results it was conjectured that most faults are activated by the baseline software program and are independent of the input sequence.

CSDL injected 21,055 faults (each pin fault was injected five times, in different locations of the program) and 3,637 (17.3 percent) were undetected. CSDL estimated that about 3000 of the undetected faults were "don't care" faults (i.e., faults on unused pins or on signals that were always low or always high under normal circumstances). Of the remainder, a few were analyzed and found to be "don't cares". In the Bendix study, 3000 faults were injected during the self-test evaluation phase and each undetected fault was analyzed. It was found that 466 faults (15.5 percent) were "don't cares" and, of these, 245 occurred in the bits of the micromemory and 47 in the control Programmable Read-Only Memory (PROM). When memory bit-faults were excluded, 7.2 percent of gate-level faults were "don't cares". Both Bendix and CSDL concluded that the identification of "don't care" faults was a non-trivial task, but essential to obtaining reasonably accurate estimates of fault coverage.

The Bendix study found that 86.5 percent of gate-level faults (excluding bit-faults in the micromemory and control PROMS) were detected during the eight repetitions of the FCS program, based on 148 injected "care" faults. Pin-level faults were not injected while executing the FCS program. The equivalent coverage in the CSDL study is not clear because of the large number of undetected, unanalyzed faults. Most of these faults (but, possibly, not all) were "don't cares." CSDL did conclude, however, that between 2 percent and 4 percent of all detected faults were detected by the background self-test programs and not by the comparators. Since self-test was not executed during the FCS experiments, Bendix would have concluded that these faults were undetected.

- The Bendix study showed that 88 percent of 2901A gate-level faults were detected during the FCS experiments, based on 52 injected "care" faults. The CSDL study gave no results for this device.

- In the Bendix study 97.4 percent of gate-level faults and 97.6 percent of pin-level faults were detected by self-test, based on 2234 and 376 injected "care" faults, respectively. The gate-level coverage excluded bit-faults in the memory elements. When these faults were included, coverage was 92 percent. The self-test program consisted of 346 Assembly Language instructions and required two to three ms to complete. The CSDL study gave no results for self-test coverage.

- The Bendix study concluded that gate-level faults were more difficult to detect than pin-level faults, especially when faults were injected into single bits of the memories. When executing software, other than the FCS, the ratio of gate-level to pin-level undetected faults was a factor of two. Unfortunately, "don't care" faults were not identified in these runs. As a result, detection coverage estimates tended to be pessimistic.

### 1.4. Conclusions

Prior to the FIIS experiments it was concluded, based upon the Bendix and CSDL studies, that:

- Most detected faults are detected within a few computational frames of their occurrence.

- The proportion of faults not detected by comparison-monitoring while executing the baseline program can range from 2 percent to 13.5 percent.

- Detection, isolation, and recovery could take up to several seconds, during which time the system (i.e., FTMP) is potentially vulnerable to second faults. The occurrence of a second fault, before the first fault is isolated, could confuse the majority vote and result in a system breakdown.

- "Don't care" faults constitute a statistically significant proportion of injected faults (between 6 percent and 17.3 percent). These faults are difficult to identify. Unidentified "don't care" faults could result in uncertain and pessimistic detection coverage estimates.

- Self-test coverage of 95 percent is easily achieved for pin-level faults and for gate-level faults if memory bit-faults are excluded.

- There is a significant difference in detection coverage between pin-level and gate-level faults, particularly if memory bit-faults are included in the latter.

# 2. OVERVIEW OF THE FIIS EXPERIMENTS

## 2.1. Objectives

The Bendix and CSDL studies were intended to provide an initial database for future FCS survivability assessment. The objectives of the FIIS experiments were (Benson, Mulcare, and Larsen, 1987):

- Corroborate and augment the results of the Bendix and CSDL studies.

- Provide a database of detection coverage and fault latency which future experimenters could use as goals or as a basis of comparison.

- Evaluate the FIIS fault injection methodology. (It was hoped that this methodology would be the first step in establishing guidelines for future fault injection experiments and fault detection coverage estimation.)

- Provide a database for the construction of single and multiple-fault models which could be used by reliability programs to assess FCS survivability.

- Identify unresolved issues associated with FCS survivability assessment and recommend studies to resolve them.

## 2.2. Test Ground Rules and Procedures

The target hardware was a dual FCC, which implemented a complete FCS for a commercial aircraft (Lockheed L-1011 Tristar). The FCS was dual/dual, but only a single pair was used in the experiments. Faults were detected by comparison monitoring of computed variables which were periodically exchanged betweⁿn FCCs. Either FCC could request and effect system disengagement if it observed a discrepancy in any of these monitored variables. System disengagement constituted "detection." In addition, the system featured haıdware comparators which were located in the secondary actuators. These comparators, which were not faulted, effectively measured the difference between the surface commands generated by the two FCCs. Again, comparator exceedances constituted "detection" and resulted in system disengagement. The experiments were conducted in open-loop and closed-loop scenarios.

### 2.2.1. Open-loop Scenario

The simulated airframe was disconnected for all runs. As a consequence, sensor inputs were invariant. In this configuration the operational program consisted of the inner loops, mode logic servicing, executive functions, synchronization, control panel and display servicing, voting and monitoring, and intercomputer communications. The open-loop program executed approximately 11,000 Assembly instructions every 50 ms.

### 2.2.2. Closed-loop Scenario

The simulated airframe was connected, including the sensor feedback signals.

In addition to the open-loop programs, the operational program consisted of the autopilot modes: cruise altitude hold, cruise climb, cruise turn, localizer capture, and glideslope capture/track. The land modes consisted of approximately 1200 additional Assembly Language instructions. In the autopilot modes the aircraft was perturbed from equilibrium flight by initial conditions and control wheel steering commands. The localizer mode was executed every 100 ms, the glideslope modes every 200 ms, and the other modes every 50 ms.

The open-loop experiments were conducted first. All faults were first injected in the open-loop scenario and only undetected faults were injected in the closed-loop scenarios. This saved time since most faults were detected in the open-loop experiments. Each undetected fault was subsequently injected during an autopilot mode, the purpose being to determine the proportion of faults detected by programs other than the baseline program. (It was assumed that the baseline program consisted of the inner-loop programs and cruise altitude hold.) The same fault was successively injected while executing each of the autopilot modes.

### 2.2.3. Self-Test

Each FCC contained a self-test program which was normally executed in the background. During the open and closed-loop experiments the self-test program was disabled. In order to determine self-test coverage and to identify "care faults", all faults which were undetected by both the open and closed-loop programs, and a larger sample of detected faults were injected separately, executing only the self-test program.

### 2.2.4. Test Conditions

Faults consisted of permanent S-a-0, S-a-1 and pin inversions, injected on input and output pins of almost every device on the data path and control cards of ᴗhe CAPS-6 computer. Devices were only excluded when they would not function with the FIIS multiplexers.

- No faults were injected in the analog interface hardware.
- Faults were injected in a single FCC of the dual pair.
- Only single faults were injected.
- Faults were detected by comparison monitoring, exclusively. Self-test was not executed in the open and closed-loop scenarios.
- No faults were injected in the hardware associated with failure detection (i.e., hardware comparators and disengage mechanisms).
- Detection was recorded at 50 ms intervals. (This was the same as the minor frame interval.)

- An undetected fault run was terminated after 15 seconds of real time (i.e., 300 open-loop iterations).

- Each fault was individually identified.

- Coverage was tabulated for unweighted and weighted faults. In the latter, faults were weighted in proportion to the failure rate of the device; in the former, all faults were weighted equally.

- All undetected faults were analyzed and "don't care" faults were eliminated from the tabulations. "Don't care" faults consisted of unused pins or signals that were always high or low under all operating conditions.

## 2.3. Results

Detailed test results can be found in Benson, Mulcare, and Larsen (1987). In this section only the results for unweighted S-a-0 and S-a-1 faults are given.

Table 2.3-1: Out of 1670 injected "care" faults, 1597 (95.63 percent) were detected and 73 (4.37 percent) were undetected. Self-test detected 1115 faults out of 1115 injected.

TABLE 2.3-1. OPEN-LOOP, UNWEIGHTED FAULTS

| Device | # Faults Injected | # Faults Detected | # Faults Undetected | Don't Cares | Percent Detected | Percent Undetected |
|---|---|---|---|---|---|---|
| Data Path | 1016 | 990 | 26 | 60 | 97.44 | 2.56 |
| Control | 654 | 607 | 47 | 63 | 92.81 | 7.19 |
| S-a-0/1 | 1670 | 1597 | 73 | 123 | 95.63 | 4.37 |
| 2901A | 283 | 283 | 0 | 13 | 100. | 0.0 |
| Micromemory | 146 | 146 | 0 | 9 | 100. | 0.0 |
| Input Pins | 1184 | 1133 | 51 | 69 | 95.69 | 4.31 |
| Output Pins | 486 | 464 | 22 | 54 | 95.47 | 4.53 |
| Self-Test | 1115 | 1115 | 0 | 0 | 100. | 0.0 |

[1] Excludes self-test

[2] Detected by self-test

[3] "Don't cares" = 6.86 percent

Table 2.3-2: Each of the 73 undetected open-loop faults was successively injected while executing each of the six autopilot modes. Thus, the same fault could have been detected while executing several modes, as indeed the results show. Of the 73 injected "care" faults, 33 (45.21 percent) were detected and 40 (54.71 percent) were undetected.

TABLE 2.3-2. CLOSED-LOOP, UNWEIGHTED FAULTS

| Mode | # Faults Injected | # Faults Detected | # Faults Undetected | Don't Cares | Percent Detected | Percent Undetected |
|---|---|---|---|---|---|---|
| Alt.Hold | 73 | 11 | 62 | 0 | 15.07 | 84.93 |
| Climb | 73 | 10 | 63 | 0 | 13.7 | 86.3 |
| Turn | 73 | 10 | 63 | 0 | 13.7 | 86.3 |
| Loc/Capt | 73 | 13 | 60 | 0 | 17.81 | 82.12 |
| GS/Capt | 73 | 9 | 64 | 0 | 12.33 | 87.67 |
| GS/Track | 73 | 12 | 61 | 0 | 16.44 | 83.56 |
| Self-Test | 73 | 73 | 0 | 0 | 100. | 0.0 |
| Totals | 73 | 33(1) | 40(1) | 0 | 45.21 | 54.79 |

[1] Detected by self-test

Table 2.3-3: These results indicate that most faults are detected while executing the baseline program. However, there is a significant number of faults not detected by either the baseline or auxiliary programs (e.g., 2.4 percent).

TABLE 2.3-3. SUMMARY OF BASELINE/AUXILIARY FAULTS

| | |
|---|---|
| Total faults injected | 1670 |
| Detected by baseline | 1597 (95.63%) |
| Undetected by baseline/detected by auxiliary | 33 (1.98%) |
| Undetected by baseline/undetected by auxiliary | 40 (2.4%) |

## 2.4. Summary of the FIIS Experiments

- Most detected faults were detected within a few computational frames of their occurrence (e.g., within 10 frames = 500 ms). This result corroborates the results of the Bendix and CSDL studies.

- Faults were activated, i.e., produced errors, primarily by the operating software and not by time-varying sensor inputs, as evidenced by the high coverage in the open-loop scenario.

- Most faults were activated (and detected) by the baseline software program (95.63 percent). This coverage is considerably better than the Bendix study indicated, which is not surprising considering that the Bendix FCS program was 2200 words whereas the open-loop program was 11,000 words.

- A small number of open-loop detected faults were detected between 1 and 6.5 seconds (0.3 percent).

- A small number of faults were not activated by the baseline program but were activated by an auxiliary program (1.98 percent).

- A small number of faults were not activated by either the baseline or auxiliary programs (2.4 percent).

- Detection statistics for weighted and unweighted faults were similar (e.g., 96.5 percent for weighted versus 95.6 percent for unweighted).

- Invert faults are less latent than stuck-ats. For example, 1.71 percent are undetected when invert faults are included versus 4.37 percent when excluded. (One-third of all faults were inverts.)

- Micromemory and 2901A faults were 100 percent detected. This is not surprising since pin-level faults on these devices tend to produce massive errors.

- Self-test coverage was 100 percent. This was impressive, even at the pin-level. The self-test designer was obviously well-acquainted with the hardware.

- The percentage of all faults classified as "don't cares" is 6.11. This is consistent with Bendix's results, which estimated 7 percent at the pin-level. The relatively large number of these faults, together with the difficulty in identifying them, precludes accurate estimates of detection coverage.

## 2.5. Conclusions of the FIIS Experiments

- FIIS test results generally corroborate the results of the Bendix and CSDL studies. This was surprising considering the dissimilarity of input sensor selection, computer architecture, and operational software between the three studies.

- The validity of the FIIS approach hinges on the validity of pin-level fault models. Until this issue is resolved the results of the FIIS and previous experiments must be considered tentative. However, the results can be used as a relative measure of fault detection capability.

- The FIIS methodology was thoroughly tested during the study. FIIS performance was impressive, especially in the following areas:

  - Fault Generation Capability: Although only stuck-at and invert faults were injected, FIIS provides the capability of simulating a wide variety of fault types.

  - Ease of Use: Injecting faults and recording data was tedious but relatively simple after the initial setup.

- Fidelity: Since faults are injected into the target hardware there is no question about the fidelity of the experiments nor is there any need to validate the simulation.

- Speed: All of the FIIS experiments were run in real time. As a consequence, it was possible and practicable to determine detection coverage over long periods of time.

# 3. FUNCTION CRITICALITY

## 3.1. Single-Fault Model

The FIIS, bendix, and CSDL studies established that, although most faults are detected within a few computational frames of their occurrence, there is a small number, perhaps 5 percent, which are not detected for much longer periods of time. These latent faults occur in devices which are infrequently exercised by the software program. As a consequence, they could accumulate and, if eventually activated by a common source of excitation, could result in a near-simultaneous loss of redundancy.

In planning the FIIS experiments, it was agreed by all of the participants that the principal and fundamental objective was to obtain a database for the reliability assessment of FCSs. As a consequence, it was necessary to anticipate the kind of data that might be required. Recognizing that the key element of a reliability assessment program was a single-fault model, it was decided to generate a strawman model in order to identify parameters which could be obtained from the FIIS experiments.

The results of the Bendix and CSDL studies seemed to indicate that most faults are activated by the baseline software (i.e., the executive and inner-loops). Only a small proportion (not activated by the baseline) are activated by auxiliary programs. These observations suggested the following definitions:

- Baseline Program: A set of continuously executed software modules.

- Auxiliary Programs: Software executed occasionally.

- Active Fault: A fault that can produce an error (for some input) while executing the current program.

- $\alpha$-Fault: A fault activated by the baseline program.

- $\beta$-Fault: A fault not activated by the baseline program.

- Benign Fault: A fault that cannot produce an error while executing the current program, regardless of input, but may produce an error for some other program.

- Latent Fault: A fault which has not yet produced a malfunction. (In the context of the single-fault model, benign and latent faults are equivalent.)

Typically the baseline program is the operating system kernel while an application program, executed on demand, would be considered an auxiliary program.

The structure of the strawman single-fault model is shown in figure 3.1-1.

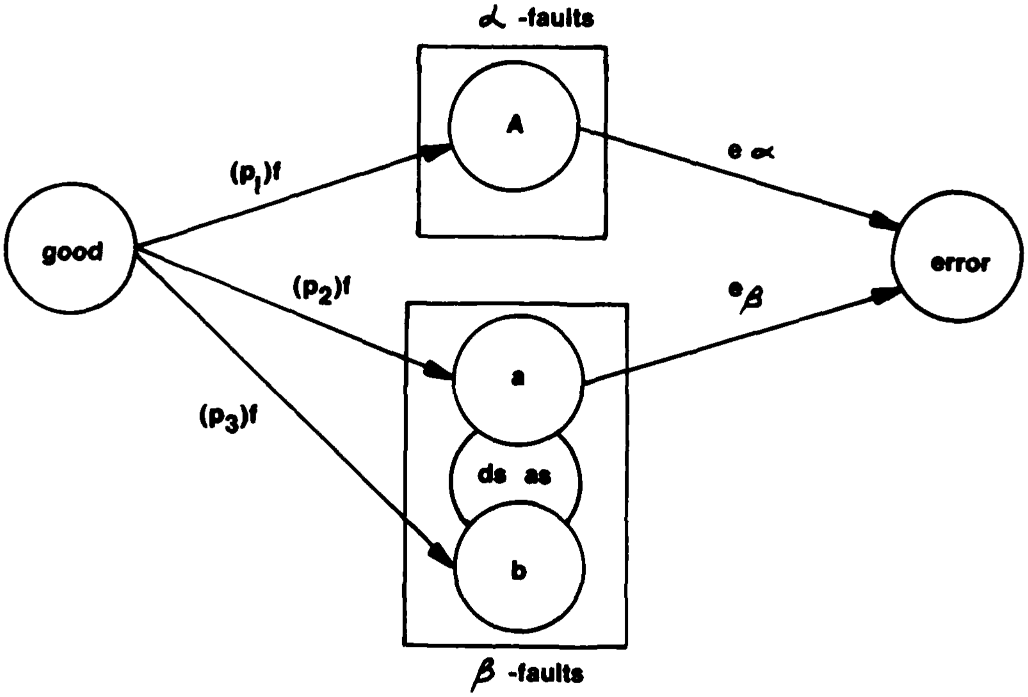


FIGURE 3.1-1. SINGLE-FAULT MODEL

The model is Markovian and appears to have sufficient degrees-of-freedom to model a wide variety of fault and error dynamics, particularly as observed in the Bendix and CSDL studies. The model is intended to model permanent faults only. The following parameters describe the fault and error dynamics:

f - failure rate of a lane (failures/hour)

$p_1$ - proportion of $\alpha$-faults

$p_2$ - proportion of $\beta$-faults which are active at their occurrence

$p_3$ - proportion of $\beta$-faults which are benign at their occurrence

$e_\alpha$ - rate at which $\alpha$-faults produce errors (errors/hour)

$e_\beta$ - rate at which $\beta$-faults produce errors (errors/hour)

as - rate at which auxiliary programs are brought online (programs/hour)

1/ds - average duration of an auxiliary program (hours/program)

q - proportion of auxiliary programs that activate a benign fault

(Henceforth, we will assume that there is only a single auxiliary program. If more than one auxiliary program were involved, the complexity of the model would increase.)

The parameters of the model are not independent. In fact,

$$p_1 + p_2 + p_3 = 1$$

$$p_2 = (1 - p_1)[\frac{as}{as + ds}]$$

$$p_3 = (1 - p_1)[\frac{ds}{as + ds}]$$

From the results of the FIIS and previous experiments it was expected to obtain estimates of $p_1$, $p_3$, $e_\alpha$, and $e_\beta$. The parameters $p_2$, as, and ds would be obtained from typical FCS scenarios (e.g., duration of and time between initiation of auxiliary programs).

### 3.2. Parameter Estimates

- $p_1$: From the Bendix study, $.85 < p_1$; from FIIS, $.96 < p_1 < .98$
- $p_2$: It is estimated that $p_2 = 0$, approximately
  (With $p_2 = 0$, $1 - p_1$ = proportion of latent faults)
- $p_3$: From the Bendix study, $p_3 < .15$; from FIIS, $.02 < p_3 < .04$
- $e_\alpha$: From the FIIS study, $e_\alpha > 7200$/hour
- $e_\beta$: From the FIIS study, $e_\beta > 900$/hour
- as: From FCS scenarios, .01/hour < as < 10/hour
- 1/ds: From FCS scenarios, .01 hours < 1/ds < 1 hour
- f: The current range is .001/hour < f < .0001/hour

### 3.3. Potential Criticality of Latent Faults

In order to assess the effects of latent faults, we present two examples of conventional FCSs which could be vulnerable to the accumulation of latent faults. The examples noted are Triplex FCS (section 3.4) and Quadruplex FCS (section 3.5). The scenario is one in which latent faults, when activated, lead to a rapid and unexpected loss of components. Such a condition can arise in a Quadruplex FCS, where for example, in time, three out of the four lanes develop latent faults. Eventually, due to a single source of excitation, such as the callup of an outer-loop program, the faults become active. Even assuming, as we do, that the time interval between the successive activation of the faults (referred to, hereafter, as "avalanching latent faults") is sufficient to allow the comparators to detect and isolate each fault in turn, the result is a loss of the three lanes in quick succession. It is our contention that the probability of such an event may not be insignificant.

3.4. Example 1 - Triplex FCS

The conventional reliability analysis, which assumes that there are no faults at the start of each flight, would conclude that the probability of loss of the FCS function in a flight of one hour is $6f^2$.

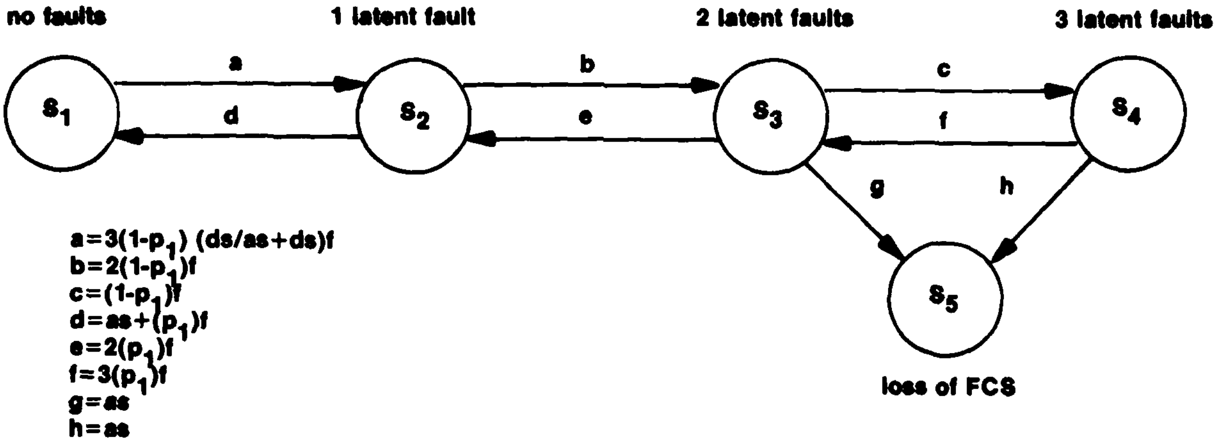


FIGURE 3.4-1. MARKOV MODEL/TRIPLEX FCS WITH LATENT FAULTS

A Markov reliability model of the FCS, representing the effects of avalanching latent faults, is shown in figure 3.4-1. The following assumptions are implicit:

- Loss of control is due, exclusively, to avalanching latent faults.
- Faults are exponentially distributed.
- The time between the successive activation of multiple latent faults is small relative to mission time.
- $\alpha$-faults (i.e., faults active at their occurrence) are detected immediately as they occur, at which time the entire lane is replaced. Thus, existing latent faults are effectively repaired.

- Excitation of latent faults is assumed to be correlated across lanes (i.e., a single excitation activates latent faults in different lanes).

Referring to figure 3.4-1:

- State $S_1$ represents the condition that all lanes are fault-free.
- State $S_2$ has a latent fault in one lane.
- State $S_3$ has a latent fault in two lanes.
- State $S_4$ has a latent fault in three lanes.
- *State $S_5$ represents loss of the FCS function.*

The transition rates are:

$$a = 3(1-p_1)f\left[\frac{ds}{as + ds}\right]$$

$$b = 2(1-p_1)f$$

$$c = (1-p_1)f$$

$$d = as + (p_1)f$$

$$e = 2(p_1)f$$

$$f = 3(p_1)f$$

$$g = as$$

$$h = as$$

It is noted that the backward transitions (d, e, and f) are the result of repairs due to the detection of $\alpha$-faults.

Let $x_1$, $x_2$, $x_3$, $x_4$, and $x_5$ denote the occupancy probabilities of states $S_1$, $S_2$, $S_3$, $S_4$, and $S_5$, respectively. From the figure we obtain the following differential equations:

$$sX_1 - x_1(0) = -aX_1 + dX_2$$

$$sX_2 = aX_1 - (b+d)X_2 + eX_3$$

$$sX_3 = bX_2 - (c+e+g)X_3 + fX_4$$

$$sX_4 = cX_3 - (f+h)X_4$$

$$sX_5 = gX_3 + hX_4$$

with initial conditions, $x_1(0) - 1$, $x_2(0) - x_3(0) - x_4(0) = x_5(0) - 0$. $X_1$, $X_2$, $X_3$, $X_4$, and $X_5$ denote the Laplace transforms of $x_1$, $x_2$, $x_3$, $x_4$, and $x_5$, respectively, and s denotes the Laplace operator.

Figure 3.4-2 shows the mean failure rate (MFR) (see appendix A), for a range of values of $1-p_1$ and f. The parameters $p_2$ and ds were fixed at the values $p_2 - 0$ and ds - 10/hour. Sensitivity studies indicate that the MFR is insensitive to values of ds between 1 and 10 per hour.

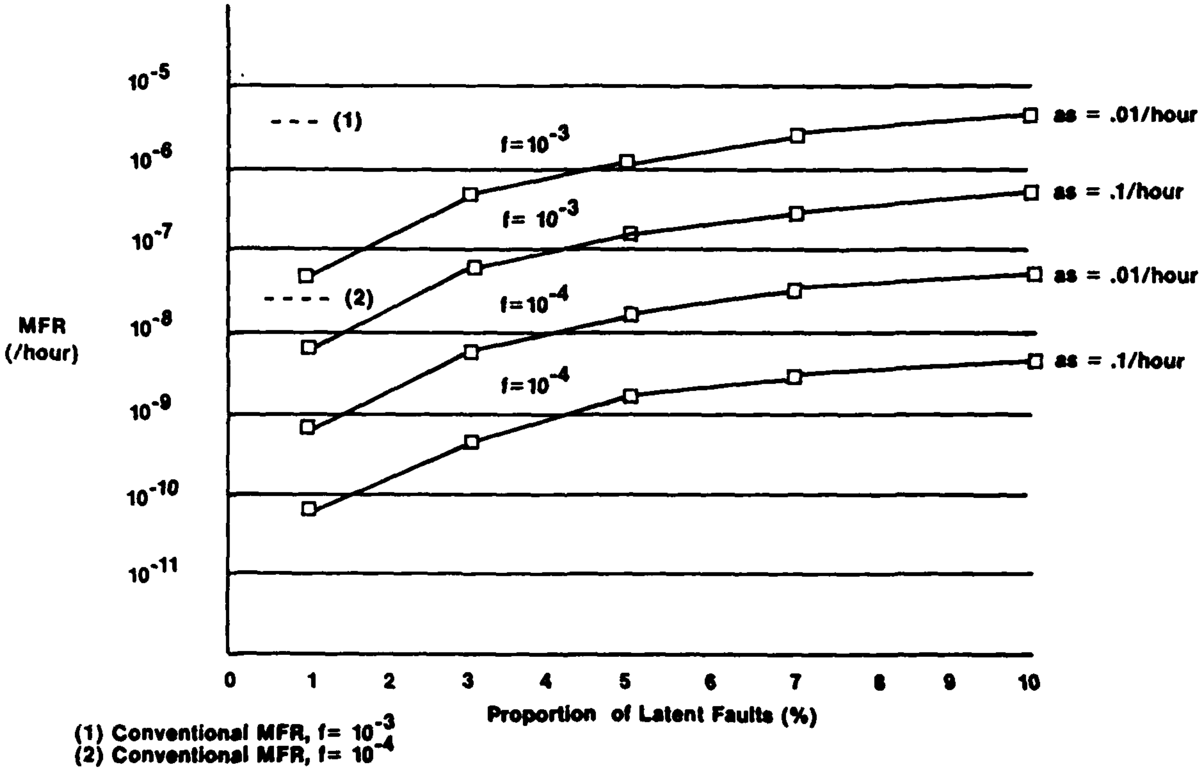


FIGURE 3.4-2. MEAN FAILURE RATE/TRIPLEX FCS

These results are summarized in tables 3.4-1 and 3.4-2 for lane failure rates ($10^{-3}$/hour and $10^{-4}$/hour, respectively). It is noted that the corresponding MFRs, based on conventional reliability analysis, are $6x10^{-6}$/hour and $6x10^{-8}$/hour, respectively.

TABLE 3.4-1. MFR, TRIPLEX FCS, f = $10^{-3}$/HOUR

| as(/hour) | $1-p_1$(%) | MFR(/hour) |
|---|---|---|
| .1 | 10 | $5.76 \times 10^{-7}$ |
| .1 | 7 | $2.82 \times 10^{-7}$ |
| .1 | 5 | $1.44 \times 10^{-7}$ |
| .1 | 3 | $5.19 \times 10^{-8}$ |
| .1 | 1 | $5.77 \times 10^{-9}$ |
| .01 | 10 | $4.47 \times 10^{-6}$ |
| .01 | 7 | $2.20 \times 10^{-6}$ |
| .01 | 5 | $1.13 \times 10^{-6}$ |
| .01 | 3 | $4.07 \times 10^{-7}$ |
| .01 | 1 | $4.53 \times 10^{-8}$ |

TABLE 3.4-2. MFR, TRIPLEX FCS, f = $10^{-4}$/HOUR

| as(/hour) | $1-p_1$(%) | MFR(/hour) |
|---|---|---|
| .1 | 10 | $5.92 \times 10^{-9}$ |
| .1 | 7 | $2.90 \times 10^{-9}$ |
| .1 | 5 | $1.48 \times 10^{-9}$ |
| .1 | 3 | $5.33 \times 10^{-10}$ |
| .1 | 1 | $5.92 \times 10^{-11}$ |
| .01 | 10 | $5.81 \times 10^{-8}$ |
| .01 | 7 | $2.85 \times 10^{-8}$ |
| .01 | 5 | $1.45 \times 10^{-8}$ |
| .01 | 3 | $5.23 \times 10^{-9}$ |
| .01 | 1 | $5.82 \times 10^{-10}$ |

### 3.4.1. Mean Failure Rate Approximation

An approximate value of MFR can be obtained as follows:

On the average, loss of control will occur if two latent faults occur in a time interval of length 1/as hours and no $\alpha$-faults occur in either of the lanes containing the latent faults. If q denotes this probability, then

$$\begin{aligned} q &\approx 6[(1-p_1)f/as]^2[1 - 2(p_1)f/as] \\ &\approx 6(1-p_1)^2 f^2 (1/as)^2 \end{aligned} \qquad (1)$$

Thus, the Mean Time to Failure (MTTF) is:

$$\text{MTTF} \approx (1/as)[\ q + 2(1-q)q + 3(1-q)^2q + \ldots\ ] \qquad (2)$$
$$= (1/as)/q$$

$$\text{MFR} \approx q(as) \qquad (3)$$
$$\approx 6(1-p_1)^2f^2/as$$

### 3.4.2. Summary of Example 1

- The relative effect of latent faults is conveniently described by the ratio

  $$R = \frac{\text{probability of loss of control with latent faults}}{\text{probability of loss of control by conventional analysis}}$$

  For values of $R << 1$, the effects of latent faults are insignificant. From the tables, the maximum value of R is .97 (for $f = 10^{-4}$, $as = .01$, $p_1 = .9$).

- Relative to the conventional MFR, a Triplex FCS does not appear to be especially vulnerable to latent faults; in the worst case, survivability is reduced by a factor of two.

- MFR is directly proportional to $(1-p_1)^2$.

- MFR is directly proportional to 1/as, the "time on risk."

- Survivability is adversely affected by the proportion of latent faults, $1 - p_1$, although for the range of parameters selected, this effect is not significant.

### 3.5. Example 2 - Quadruplex FCS

The conventional reliability analysis would indicate that probability of loss of the FCS function in a flight of one hour = $24f^3$.

A Markov reliability model of the FCS is shown in figure 3.5-1. The assumptions are the same as for the triplex system.

Referring to figure 3.5-1:

- State $S_1$ represents the condition that all lanes are fault-free.

- State $S_2$ has a latent fault in one lane.

- State $S_3$ has a latent fault in two lanes.

- State $S_4$ has a latent fault in three lanes.

- State $S_5$ has a latent fault in four lanes.

- State $S_6$ represents loss of the FCS function.

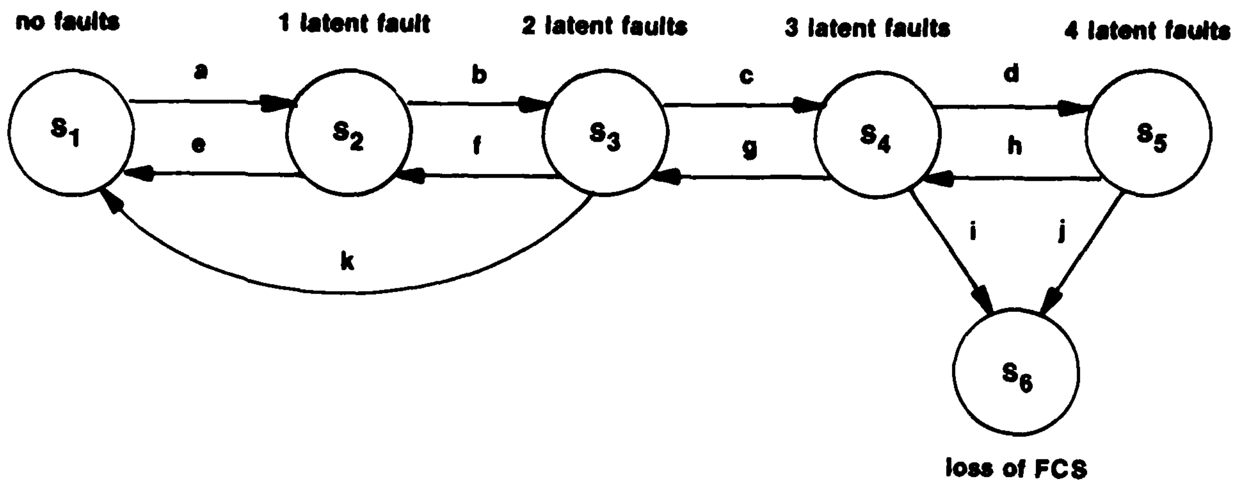


FIGURE 3.5-1. MARKOV MODEL/QUADRUPLEX FCS WITH LATENT FAULTS

The transition rates are:

$$a = 4(1-p_1)f[\frac{ds}{as + ds}]$$

$$b = 3(1-p_1)f$$

$$c = 2(1-p_1)f$$

$$d = (1-p_1)f$$

$$e = as + (p_1)f$$

$$f = 2(p_1)f$$

$$g = 3(p_1)f$$

$$h = 4(p_1)f$$

$$i = as$$

$$j = as$$

$$k = as$$

Again, it is noted that the backward transitions (e, f, g, h, and k) are the result of repairs due to the detection of $\alpha$-faults.

From the figure we obtain the following differential equations:

$$
\begin{aligned}
sX_1 - x_1(0) &= -aX_1 + eX_2 + kX_3 \\
sX_2 &= aX_1 - (b + e)X_2 + fX_3 \\
sX_3 &= bX_2 - (c + f + k)X_3 + gX_4 \\
sX_4 &= cX_3 - (d + g + i)X_4 + hX_5 \\
sX_5 &= dX_4 - (h + j)X_5 \\
sX_6 &= iX_4 + jX_5
\end{aligned}
$$

with initial conditions, $x_1(0) = 1$, $x_2(0) = x_3(0) = x_4(0) = x_5(0) = x_6(0) = 0$. $X_1$, $X_2$, $X_3$, $X_4$, $X_5$, and $X_6$ denote the Laplace transforms of $x_1$, $x_2$, $x_3$, $x_4$, $x_5$, and $x_6$, respectively.

Figure 3.5-2 shows the MFR for a range of $1-p_1$ and f with $p_2$ and ds again fixed at $p_2 = 0$, ds = 10/hour. These results are summarized in tables 3.5-1 and 3.5-2 for lane failure rates, $10^{-3}$/hour and $10^{-4}$/hour, respectively.

It is noted that the corresponding MFRs, based on conventional reliability analysis, are $2.4 \times 10^{-8}$/hour and $2.4 \times 10^{-11}$/hour, respectively.

TABLE 3.5-1. MFR, QUADRUPLEX FCS, F = $10^{-3}$/HOUR

| as(/hour) | $1-p_1$(%) | MFR(/hour) |
|---|---|---|
| .1 | 10 | $2.23 \times 10^{-9}$ |
| .1 | 5 | $2.80 \times 10^{-10}$ |
| .1 | 3 | $6.04 \times 10^{-11}$ |
| .1 | 1 | $2.24 \times 10^{-12}$ |
| .01 | 10 | $1.37 \times 10^{-7}$ |
| .01 | 5 | $1.73 \times 10^{-8}$ |
| .01 | 3 | $3.75 \times 10^{-9}$ |
| .01 | 1 | $1.39 \times 10^{-10}$ |

TABLE 3.5-2. MFR, QUADRUPLEX FCS, F = $10^{-4}$/HOUR

| as(/hour) | $1-p_1$(%) | MFR(/hour) |
|---|---|---|
| .1 | 10 | $2.36\text{x}10^{-12}$ |
| .1 | 5 | $2.95\text{x}10^{-13}$ |
| .1 | 3 | $6.38\text{x}10^{-14}$ |
| .1 | 1 | $2.37\text{x}10^{-15}$ |
| .01 | 10 | $2.25\text{x}10^{-10}$ |
| .01 | 5 | $2.82\text{x}10^{-11}$ |
| .01 | 3 | $6.1\ \text{x}10^{-12}$ |
| .01 | 1 | $2.26\text{x}10^{-13}$ |

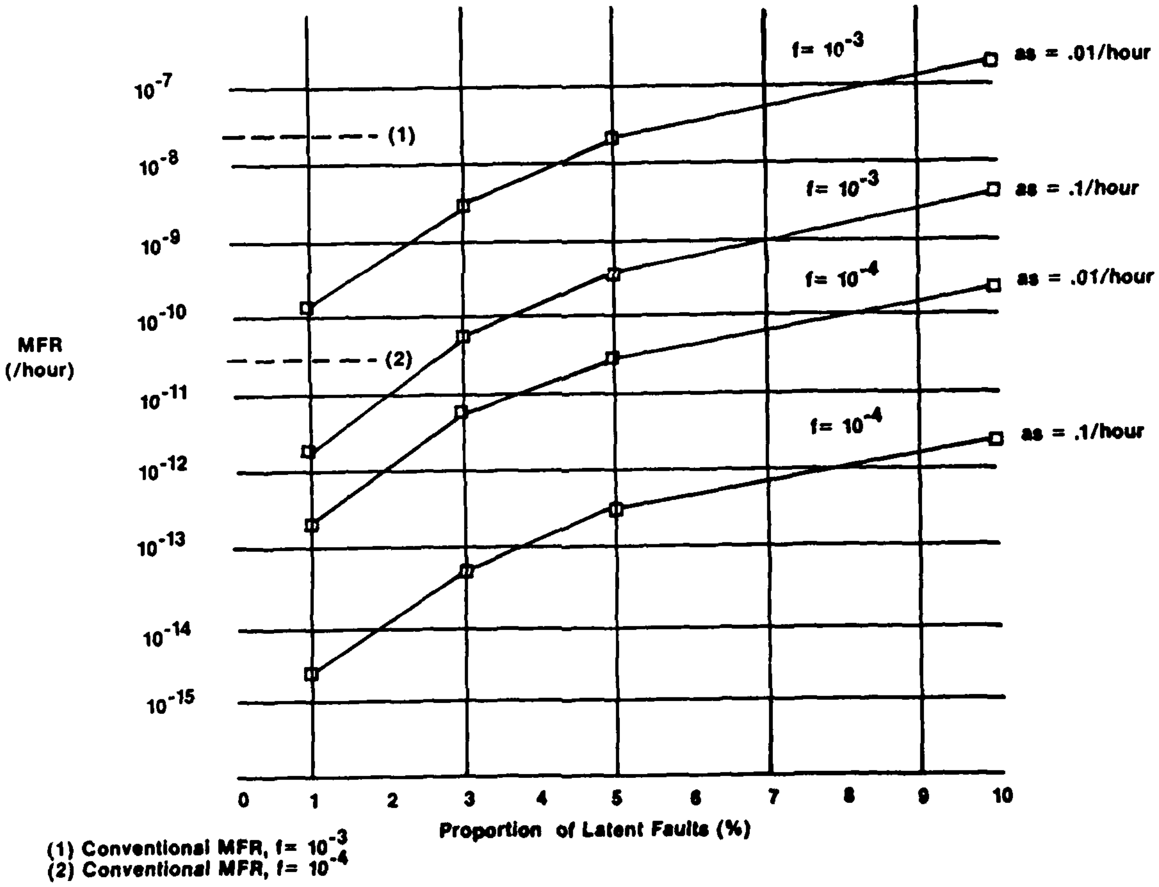


FIGURE 3.5-2. MEAN FAILURE RATE, QUADRUPLEX FCS

### 3.5.1. Mean Failure Rate Approximation

An approximate value of MFR for the Quadruplex FCS can be obtained as follows:

On the average, loss of control will occur if three latent faults occur in a time interval of length 1/as hours and no $\alpha$-faults occur in any of the lanes containing the latent faults. If q denotes this probability, then

$$\begin{aligned} q &\approx 24[(1-p_1)f/as]^3[1 - 3(p_1)f/as] \\ &\approx 24(1-p_1)^3f^3/as^3 \end{aligned} \tag{4}$$

$$\begin{aligned} MTTF &\approx (1/as)[\ q + 2(1-q)q + 3(1-q)^2q + \ldots] \\ &= (1/as)/q \end{aligned} \tag{5}$$

$$\begin{aligned} MFR &\approx q(as) \\ &\approx 24(1-p_1)^3f^3/as^2 \end{aligned} \tag{6}$$

### 3.5.2. Summary of Example 2

- For the range of parameters selected, the maximum value of R is 10 ($f = 10^{-4}$, $as = .01$, $p_1 = .9$), indicating that latent faults could have a significant effect on survivability.

- Relative to the conventional MFR, a Quadruplex FCS is more vulnerable to latent faults than a Triplex FCS.

- MFR is directly proportional to $(1-p_1)^3$.

- MFR is directly proportional to $(1/as)^2$. Thus, for example, increasing the "time on risk", 1/as, by a factor of 10 increases the MFR by a factor of 100.

### 3.6. Self-Test

From the preceding examples, it is apparent how self-test can reduce the degrading effects of latent faults: by reducing the proportion of latent faults, $1-p_1$. If it is assumed that self-test coverage of $\alpha$- and $\beta$-faults is the same, then if 1-u denotes self-test coverage, the proportion of latent faults can be reduced to $u(1-p_1)$. In the Triplex FCS a self-test coverage of only 90 percent reduces the MFR by a factor of 100 and, in the Quadruplex FCS, by a factor of 1000.

# 4. UNRESOLVED ISSUES

Although the Bendix, CSDL, and FIIS studies have contributed significantly to our understanding of fault, error, and detection dynamics, a number of important issues connected with FCS survivability assessment remain unresolved.

- Failure Modes of Digital Devices

  Previous fault injection experiments have employed stuck-at faults either on device pins or on internal gate nodes. It remains to be determined to what extent stuck-at faults represent failure modes of real devices.

- Pin-Level Versus Gate-Level Faults

  Until actual failure mode data becomes available, experimenters will, no doubt, continue to inject pin-level and gate-level faults. The Bendix study indicated a significant difference between pin-level and gate-level detection coverage At issue is the validity of either fault type and the extent to which one is more or less latent than the other.

- Single-Fault Model Incorporating Intermittent/Transient Faults

  The single-fault model of figure 3.1-1 appears to be adequate for permanent faults. The model should be extended to include intermittent and transient faults. Estimates of occurrence, duration, and reoccurrence rates are required.

- Effects of Periodic Maintenance

  Periodic maintenance can have a significant effect on reducing latent faults to acceptable levels. Unfortunately, incorporating maintenance effects in reliability models leads to computational difficulties. McGough, Reibman, and Trivedi (to be published) offers one approach to this problem.

- Multiple-Fault Models

  In order to perform a reliability assessment of an FCS it is essential to model multiple fault effects. The multiple-fault models of figures 3.4-1 and 3.5-1 are too rudimentary to be of general use. Required is a more comprehensive multiple-fault model which includes the correlation of latent faults across different lanes.

# 5. SUPPLEMENTAL WORKED EXAMPLE

In the two examples of section 3, the assessment of latent faults was based on several assumptions e.g., the structure of the single-fault model and the correlation of excitation across different lanes.

In this section another perspective of the effects and potential criticality of latent faults on aircraft survivability is presented.

In general, the effects and criticality of latent faults are dependent upon the detailed FCS design, in particular, the levels of redundancy and the fault detection, isolation, and recovery mechanisms employed. As a consequence, the strawman FCS selected for this example should not be construed as being typical or even representative of FCSs. It was selected for the following reasons:

- It is a realistic FCS; similar configurations have been used in the past.
- The associated fault and reliability models are relatively simple and easily understood; the state occupancy probabilities can be obtained analytically.

## 5.1. FCS Configuration

The FCS is required to increase the fatigue life of the aircraft. This is achieved by improving the damping of the short period and dutch roll modes and controlling the phase of one or two bending modes. The aircraft, however, is controllable without the FCS. Thus, loss of the FCS function does not, in any way, impair the safety of the vehicle. However, an undetected fault could result in an unsafe condition. Thus, it is a firm requirement that such faults be precluded, at least to a probability of $10^{-7}$/hour, the generally accepted goal for military aircraft.

The FCS configuration is shown in figure 5.1-1. Referring to the figure:

- The FCS consists of two independent lanes, each containing a processor (P) and dedicated disengage logic (Q and associated relay).
- Each processor drives a different actuator.
- Each processor receives information from an independent set of sensors.
- Each processor computes the commands for its own and the other actuator and compares both commands with those of the other processor. This data is exchanged via the intercomputer data links. Any observed difference, exceeding a comparator threshold, will cause that processor to send a discrete to both $Q_1$ and $Q_2$, opening the relays and disengaging both actuators.

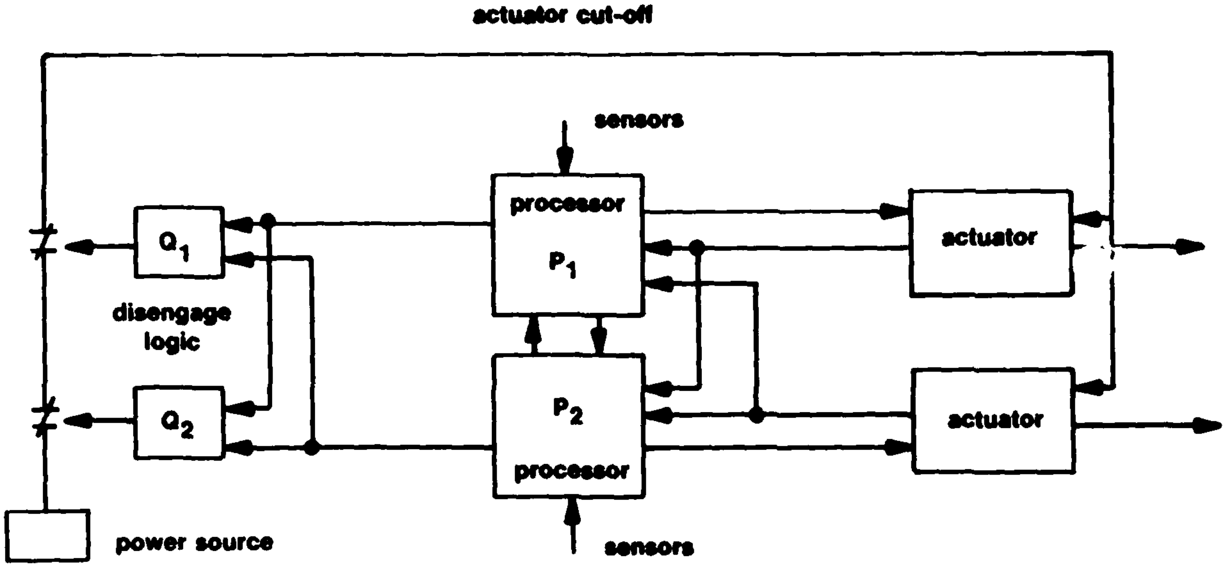


FIGURE 5.1-1. DUAL, FAIL SAFE FLIGHT CONTROL SYSTEM

## 5.2. Unsafe Condition

An unsafe condition can arise only if a processor fails and it and the non-failed processor are unable to disengage the actuators. Such an event could only occur if both disengage elements, $Q_1$ and $Q_2$, have failed previously. In practice, the disengage logic would be tested in preflight test. The issue is, what level of failure detection coverage is required?

## 5.3. Repair of Latent Faults

In generating the reliability model it must be determined when and how latent faults are repaired. In this example it is assumed that a detected fault will result in the replacement of the entire lane, both processor and disengage logic, by non-faulted components.

## 5.4. Markov Reliability Model

The reliability model of the FCS is shown in figure 5.4-1. The following assumptions are implicit:

- The model only includes the effects of latent faults.
- Faults are exponentially distributed.
- Mission duration is small relative to the mean time between failures.

- All faults in the disengage logic, $Q_1$ and $Q_2$, are latent (i.e., they produce no effects until a fault in $P_1$ or $P_2$ occurs).

- Any fault in the disengage logic prevents disengagement via the associated relay.

- All faults in the processors are detected immediately as they occur at which time the entire lane is replaced.

- A fault, undetected by preflight test, will remain undetected no matter how often the test is executed.

- All faults in $P_1$ and $P_2$ ar: detected by preflight test.

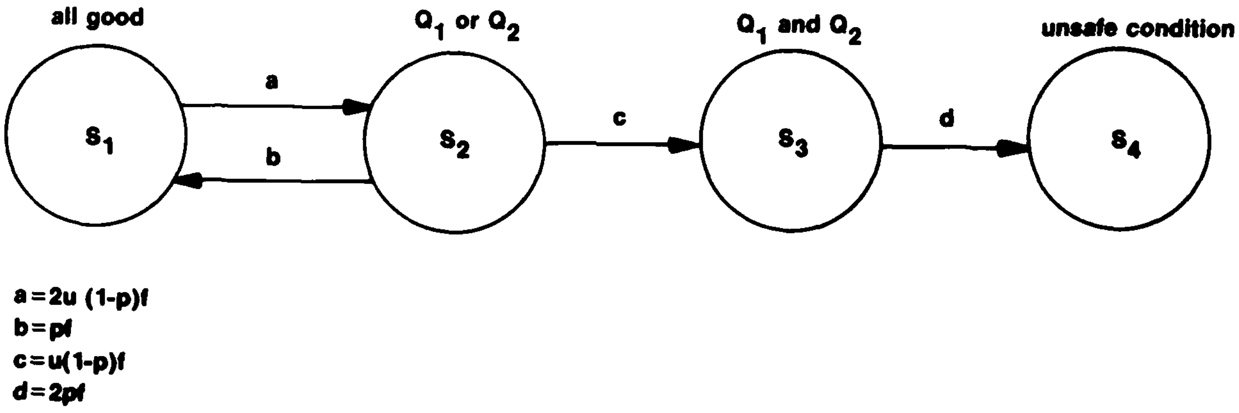


FIGURE 5.4-1. MARKOV MODEL/DUAL, FAIL SAFE, FLIGHT CONTROL SYSTEM

Referring to figure 5.4-1:

- State $S_1$ represents the condition that all lanes are fault-free.

- State $S_2$ represents the condition of a latent fault in $Q_1$ or $Q_2$ but not both.

- State $S_3$ represents the condition of latent faults in both $Q_1$ and $Q_2$.

- State $S_4$ represents the unsafe condition.

- A transition from $S_1$ to $S_2$ occurs when a fault occurs in $Q_1$ or $Q_2$.

- A transition from $S_2$ to $S_1$ occurs if $Q_1$ ($Q_2$) fails and $P_1$ ($P_2$) fails subsequently. Thus, the latent fault is repaired.

- A transition from $S_2$ to $S_3$ occurs when a second logic element fails.

- A transition from $S_3$ to $S_4$ occurs when both $Q_1$ and $Q_2$ have failed and a processor fails subsequently.

### 5.4.1. Model Parameters

- f = failure rate of a lane (failures/hour)

- pf = failure rate of a processor (failures/hour)

- (1-p)f = failure rate of the disengage logic (failures/hour)

- u = proportion of faults in the disengage logic not detected by pre-flight test

- $a = 2u(1-p)f$

- $b = pf$

- $c = u(1-p)f$

- $d = 2pf$

- 1-p = proportion of faults in the disengage logic

- p = proportion of faults in the processor, $P_1$ or $P_2$

Typical parameter values are

$$10^{-4}/\text{hour} < f < 10^{-3}/\text{hour}$$

$$.9 < p < 1$$

$$.9 < u < 1$$

### 5.5. Effects of Latent Faults on Survivability

Let $x_1$, $x_2$, $x_3$, and $x_4$ denote the occupancy probabilities of states $S_1$, $S_2$, $S_3$, and $S_4$, respectively. From the figure we obtain the following differential equations:

$$sX_1 - x_1(0) = -aX_1 + bX_2$$

$$sX_2 = aX_1 - (b+c)X_2$$

$$sX_3 = cX_2 - dX_3$$

$$sX_4 = dX_3$$

with initial conditions, $x_1(0) = 1$, $x_2(0) = x_3(0) = x_4(0) = 0$. $X_1$, $X_2$, $X_3$, and $X_4$ denote the Laplace transforms of $x_1$, $x_2$, $x_3$, and $x_4$, respectively, and s denotes the Laplace operator.

We could solve for $x_4(t)$, the probability of an unsafe condition, analytically, as a function of time. Instead, we compute the MFR. As shown in Appendix A:

$$\text{MTTF} = -\lim_{s\to 0} sX_4(s)/ds \tag{7}$$

We can solve directly to obtain

$$X_4(s) = \frac{acd}{s(s + d)(s^2 + (a + b + c)s + ac)} \tag{8}$$

$$\text{MTTF} = \frac{ac + d(a + b + c)}{acd} \tag{9}$$

$$\begin{aligned} \text{MFR} &= \frac{acd}{ac + d(a + b + c)} \\ &= \frac{4u^2p(1-p)^2f}{2u^2(1-p)^2 + 2p[3u(1-p) + p]} \end{aligned} \tag{10}$$

Setting $v = u\left(\frac{1-p}{p}\right)$,

$$\text{MFR} = \frac{2v^2pf}{v^2 + 3v + 1} \quad (\approx 2v^2pf) \tag{11}$$

## 5.6. The Conventional Reliability Analysis

The conventional reliability analysis assumes that no faults exist at the start of a flight. In this case, an unsafe condition can occur if and only if $Q_1$ and $Q_2$ both fail and $P_1$ or $P_2$ fails subsequently. Assuming a one-hour flight, this probability is given by

$$\begin{aligned} q &= (1-p)^2f^2(2pf)/6 \\ &= p(1-p)^2f^3/3 \end{aligned} \tag{12}$$

This event is order-dependent (i.e., $Q_1$ and $Q_2$ must both fail before $P_1$ or $P_2$). It can be shown that the order of occurrence is equiprobable if the flight time is small relative to 1/f. There are 12 possible orderings of $Q_1$, $Q_2$, $P_1$, and $P_2$, taken three at a time, but only four result in an unsafe condition, for example, $(Q_1,Q_2,P_1)$, $(Q_1,Q_2,P_2)$, $(Q_2,Q_1,P_1)$, $(Q_2,Q_1,P_2)$.

Employing Bernoulli trials, the mean time to first failure (i.e., an unsafe condition) is

$$\text{MTTF} = 1/q$$

and, thus,

$$\begin{aligned} q &= \text{MFR} \\ &\approx p(1-p)^2 f^3/3 \end{aligned} \tag{13}$$

Comparing (11) and (13) it can be seen that the MFR, due exclusively to latent fault conditions, is proportional to f whereas the conventional MFR is proportional to f cubed.

## 5.7. Numerical Example

To assess the relative effects of latent fault accumulation on system survivability we give several numerical examples, assuming $p = .95$ and $f \approx 10^3$/hour.

Case 1. No preflight test (i.e., $u \approx 1$).

$$\text{MFR(latent)} = 4.53\text{x}10^{-6}/\text{hour}.$$

Case 2. Preflight test with $u = 0.1$ (90 percent fault detection coverage).

$$\text{MFR(latent)} = 4\text{x}10^{-8}/\text{hour}.$$

In contrast, the conventional MFR is

$$\text{MFR(conventional)} = 7.91\text{x}10^{-13}/\text{hour}.$$

## 5.8. Summary of Example

From this simple example, it can be seen that the accumulation of latent faults can have a profound effect on system survivability. In fact, they are often the dominant cause of system loss. As a consequence, it is incumbent on the system designer to assess the vul erability of the FCS to such faults and, if significant, establish self-test coverage requirements accordingly.

# 6. CONCLUSIONS

In the Introduction, four questions were raised in connection with latent faults. As the examples given in this tutorial illustrate, the answers depend upon the details of the FCS design, the levels of redundancy, the fault detection, isolation, and recovery mechanisms employed, and the survivability goals of the FCS. As a consequence, we venture to give some answers but only with respect to the FCSs presented in this tutorial.

- What proportion of faults are latent?

  In the FCSs used in the Bendix, CSDL, and FIIS experiments the proportion of latent faults ranged between 2 percent and 15 percent. A less pessimistic estimate, based on the FIIS experiments, indicates a range between 2 percent and 4 percent. In the FCS of section 5, the proportion is a function of the relative failure rate of the disengage logic.

- What mechanisms activate latent faults?

  Latent faults are activated when the faulty components are exercised. In the systems used in the Bendix, CSDL, and FIIS experiments latent faults appear to be activated primarily by software programs. In the FCS of section 5, latent faults are activated when faults occur in other components.

- What are the effects of latent faults on aircraft survivability?

  In the two examples of section 3 these effects are given in figures 3.4-2 and 3.5-2. In the FCS of section 5 these effects are given by equation (10). Obviously, the effects of latent faults are highly dependent on the FCS configuration. In any case, their significance can only be evaluated relative to the survivability goal of the FCS. (In the examples given, this goal was assumed to be the survivability as determined by conventional analysis.)

- If latent faults are a contributing factor to reduced survivability, what level of coverage is required to detect and eliminate them?

  In the examples given in sections 3 and 5, a modest coverage could reduce these effects to insignificance (e.g., a 90 percent coverage will improve survivability by several orders of magnitude).

# APPENDIX A - MEAN FAILURE RATE

## Occupancy Probability

A homogeneous Markov model is described by a set of linear differential equations of the form

$$dx/dt = Ax \tag{1}$$

where

$A = (a_{ij}) = nxn$, is a constant matrix of transition rates, and

$x = col(x_1, x_2, \ldots, x_n)$, is a vector of occupancy probabilities of states S1, S2,..., Sn, respectively.

In most FCS reliability models there is exactly one absorbing state, the loss of control state, which we designate as $S_n$. The associated occupancy probability, $x_n(t)$, is then a cumulative distribution function and can be expressed in the form

$$dx_n(t)/dt = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn-1}x_{n-1} \tag{2}$$

In many cases, $x_n(t)$ is not a convenient measure of survivability. For example:

- For models with large numbers of states or models which contain cyclic paths (Marie, Reibman, and Trivedi, 1987), the computation of $x_n(t)$ requires the aid of a reliability analysis program such as ARIES, CARE III and HARP.
- In the conventional reliability model the FCS is assumed to be completely repaired at the start of each flight. Thus, the probability of loss of control during the first flight is the same for all flights. When latent faults are present, however, the FCS may only be partially repaired at the start of a flight. Consequently, the probability of loss of control is different for each flight, tending to increase with time. In these scenarios the occupancy probability of loss of control is not a practicable measure of survivability because it requires a recursive solution of the Markov model over a large number of flights.

We propose an alternate measure of survivability, called MFR. The MFR is defined as the reciprocal of the MTTF (McGough, Reibman, and Trivedi [to be published]).

The advantages of the MFR criteria are as follows:

- It is relatively easy to compute, even for models with cyclic paths, requiring only solutions of linear, algebraic equations.

- It is independent of time.
- It characterizes survivability over the life of the airplane.
- It provides a relative measure of survivability even if rejected as an absolute measure.

The disadvantage of MFR is that it gives no indication of how survivability degrades with time.

Computation of Mean Failure Rate

Taking the Laplace transform of both sides of equation (2) gives, for $x_n(0) = 0$,

$$sX_n(s) = a_{n1}X_1(s) + a_{n2}X_2(s) + \ldots + a_{nn-1}X_{n-1}(s) \tag{3}$$

where

$X_k(s)$ is the Laplace transform of $x_k(t)$ and s is the Laplace operator.

Using the moment generating property of Laplace transforms:

$$\begin{aligned} MTTF &= -\lim_{s\to 0} sdX_n(s)/ds \\ &= -[an1X_1'(s) + an2X_2'(s) + \ldots, +ann\text{-}1X_{n-1}'(s)] \end{aligned} \tag{4}$$

where the prime denotes the derivative with respect to s.

If we let $X(s) = \text{col}\ [X_1(s), X_2(s), \ldots, X_n(s)]$, equation (1) can be expressed as

$$sX(s) - x(0) = AX(s) \tag{5}$$

Differentiating both sides of equation (5), we obtain

$$X(s) + sX'(s) = AX'(s) \tag{6}$$

Setting s = 0 gives

$$X(0) = AX'(0) \tag{7}$$

The quantities $X_1(0)$, $X_2(0)$, ..., $X_{n-1}(0)$ are obtained by setting s = 0 in equation (5) and solving the resultant linear system by using the method of Gaussian elimination or an iterative method like Gauss-Seidel. Substituting these values into the first n-1 equations in (7) we can solve for $X_1'(0)$, $X_2'(0)$, ..., $X_{n-1}'(0)$. A unique solution exists because $S_n$ is the only absorbing state. The resulting values $X_1'(0)$, $X_2'(0)$, ..., $X_{n-1}'(0)$ are substituted into equation (4) to obtain the MTTF. Then

MFR = 1/MTTF.

## BIBLIOGRAPHY

Benson, W., Mulcare, D., and Larsen, W., Hardware Fault Insertion and Instrumentation System: Experimentation and Results, DOT/FAA/CT-86/34, FAA Technical Center, March 1987.

Lala, J. and Smith, T. B., Development and Evaluation of a Fault-Tolerant Multiprocessor (FTMP) Computer - Volume III, FTMP Test and Evaluation, NASA CR 166073, NASA Langley Research Center, May 1983.

Marie, R. A., Reibman, A. L., and Trivedi, K. S., Transient Solution of Acyclic Markov Chains, Performance Evaluation, Vol.7, No.3, 1987, pp. 175-194.

McGough, J. G., Reibman, A. L., and Trivedi, K. S., "Markov Reliability Models for Digital Flight Control Systems," AIAA Journal of Guidance and Control (to be published).

McGough, J. G. and Swern, F., Measurement of Fault Latency in a Digital Avionic Processor, Part II, NASA CR 3651, NASA Langley Research Center, January 1983.

## GLOSSARY

AVALANCHING LATENT FAULTS. The successive activation of latent faults.

MEAN FAILURE RATE. A measure of survivability defined as the reciprocal of the mean time to system failure.

BASELINE PROGRAM. A set of continuously executed software modules.

AUXILIARY PROGRAMS. Software executed occasionally.

ACTIVE FAULT. A fault that can produce an error (for some input) while executing the current program.

$\alpha$-FAULT. A fault activated by the baseline program.

$\beta$-FAULT. A fault not activated by the baseline program.

BENIGN FAULT. A fault that cannot produce an error while executing the current program, regardless of input, but may produce an error for some other program.

LATENT FAULT. A fault which has not yet produced a malfunction. (In the context of the single-fault model, benign and latent faults are equivalent.)

## ACRONYMS AND ABBREVIATIONS

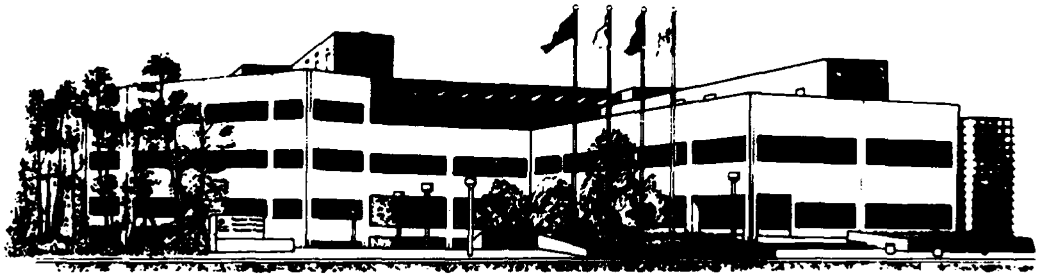
| | |
|---|---|
| ALU | Arithmetic Logic Unit |
| BGU | Bus Guardian Unit |
| CPU | Central Processing Unit |
| CSDL | Charles Stark Draper Laboratories |
| FCC | Flight Control Computers |
| FCS | Flight Control System |
| FIIS | Fault Insertion and Instrumentation System |
| FTMP | Fault-Tolerant Multiprocessor |
| GS | Glideslope |
| I/O | Input/Output |
| MFR | Mean Failure Rate |
| ms | Millisecond |
| MTTF | Mean Time to Failure |
| P | Processor |
| PROM | Programmable Read-Only Memory |
| RAM | Random Access Memory |
| ROM | Program Memory |
| S-a-0 | Stuck at Zero |
| S-a-1 | Stuck at One |
| TMR | Triple Modular Redundant |

U.S. Department of Transportation
Federal Aviation Administration

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II DIGITAL SYSTEMS VALIDATION

## CHAPTER 11
## AIRCRAFT ELECTROMAGNETIC COMPATIBILITY (GUIDELINES TO ASSESS EMC DESIGNS)



PREPARED BY:

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

PREPARED FOR:

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

## PREFACE

This document is based on work performed by the Boeing Commercial Airplane Company, P.O. Box 3707, Seattle, Washington 98124, under the National Aeronautics and Space Administration (NASA) contract NASA-12261 for the Federal Aviation Administration (FAA), NASA-Ames Research Center, Moffett Field, California 94035. The contract was firm fixed price, level-of-effort term from September 1985 to September 1986 with an extension to June 1987. Contracting officers were W. C. Botts, Boeing and A. N. Johnson, NASA. The FAA contracting officer's technical representative (COTR) was William E. Larsen. Deliverables were an Interim Report (Draft) and an Interim Report (Final). The program manager was Robert D. Force, and principal investigator, Clifton A. Clarke.

Bob Force, who helped put the program together, played a central part in managing the planning and organization of the total document. The section 2.1, "Existing Systems," is derived from the valuable "Active Controls Technology" report which Bob co-authored. Bill Larsen provided extensive expertise taken from his own experience, and through constructive source material. He also provided sound and highly regarded recommendations for content and organization. Dale R. Reed collaborated on the wiring-induced voltages and worked some of the in-depth computations. He offered very profitable perspectives on the approach to aircraft engineering analysis and design; his forbearance and tenacity are appreciated.

Special contributions were made by John Tinner and John Bishop who consulted on significant aircraft test and troubleshooting procedures, helping to fill in the picture of aircraft electromagnetic interference. Veteran EMC engineers who supplied valued and time-tested data that form a part of this report were Jerry Carter, John Foster, and George Ketterling. Thanks are also due those individuals mentioned or quoted in the text.

Many people contributed important comments and helpful criticisms to the Interim Report (Draft). Chris Kendall supplied valuable consultations and comments along with Roger McConnell of CKC Associates. Henrietta Gilbert, FAA; Richard Hess, Sperry Corp.; Russell Carstensen, Naval Air Systems Command; and Kary Miller of Collins generously took time to review and comment with useful corrections and suggestions. My thanks are also owed to Nancy Clarke for helpful editorial comments. Fellow EMC engineers Glenn Olson, Kieth Kalanquin, Charles King, and Sy O'Young (who worked on the proposal) contributed their thoughts.

The document format and graphics were expertly delineated by Primo Mattieligh and drawn by Irene Ohashi. Their generosity and patience are much appreciated. Gary Breidenstein offered expert aid in the editing and was a source of inspiration in the preparation of the final copy. Nancy Eaton not only supervised the typing but helped proof the manuscript.

This document would not be possible without the unparalleled IEEE Symposium Records and the periodical "ITEM", R & B Enterprises, whose presentations were a source of valuable data applicable to an aircraft.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

# LIST OF ILLUSTRATIONS

## LIST OF ILLUSTRATIONS (Continued)

## LIST OF ILLUSTRATIONS (Continued)

Figure Page

## LIST OF TABLES

Table Page

# EXECUTIVE SUMMARY

The Aircraft Electromagnetic Compatibility guidelines document deals with electromagnetic compatibility in a commercial transport aircraft including the specifications, the activities, the design, and the tests to verify and validate compatibility.

Objectives are to view architecture, equipment and wiring location, material properties, circuit susceptibilities, and environment as seen from the electromagnetic compatibility design perspective of balanced circuits, filters, electrical bonding, grounding, and shielding.

Even today, digital electronics are much more common in aircraft. Automated flight controls of future aircraft will operate under the control of digital clocks, data buses, switching regulators, pulse width modulated power, and radio frequency transmitters on the one hand, and on the other, sensitive analog and digital instrumentation.

Safe and efficient flight will depend on the performance of electronics. It will be important to understand the electromagnetic interference types and the electromagnetic interference paths (figure E-1).

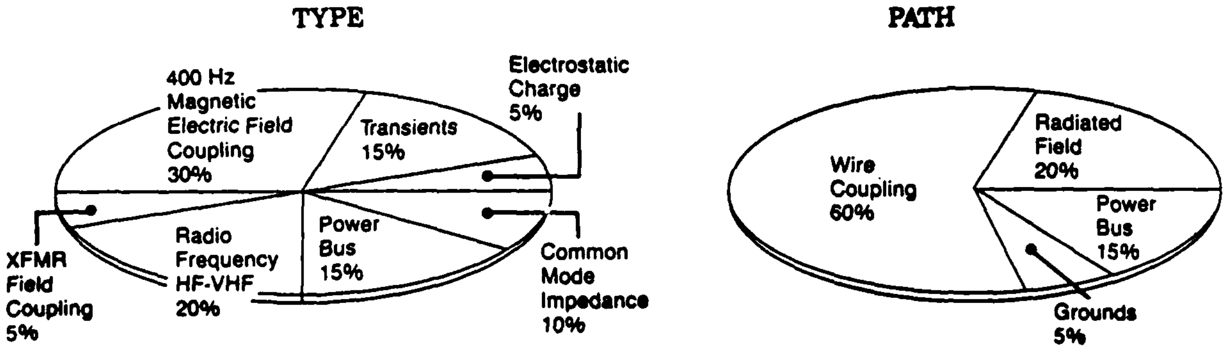


FIGURE E-1. POSTULATED PERCENTAGES

The Electromagnetic Interference (EMI) types are set forth in this document by showing a profile of the magnetic and electric fields from power lines; some military, urban, and rural radio frequency field strengths; and the properties of transients. Significance of the wire circuit return, the balanced circuit, grounding, shielding, and software highlight the protection techniques of a layered design which will block paths of electromagnetic interference and maintain interface signal quality. Design specifications, activities, and reviews are proposed to help set up guidelines for equipment verification and aircraft validation.

# 1. INTRODUCTION

## 1.1. Background and Scope

### 1.1.1. A Case of Engine Shutdown

Captain Hoag thought briefly of the moment when he left home last night. His son, daughter, and wife were all there. They had joked about their planned upcoming vacation, their first together in two years.

A voice broke into his short reverie: "Flight 211, you're low and to the left - please maintain 023 - you have a cell at 2 o'clock."

Hoag said to the first officer, John Pearson: "John, push it forward and bring 'er up."

John said: "Gotcha covered. I flew one of these new ones two weeks ago into Loridan International - they sure do handle smoothly."

"Okay - uh huh." "Gear down."

Flight 211, Atlantic Air, was on approach to Keithrode International Airport (KIA). It was 16:45 on October 16. Two hundred and twenty-seven passengers were on board. The weather had been partly cloudy with thunderstorms predicted and cell activity in the proximity of the air terminal.

Tower: "Flight 211, you are cleared on Runway 3. You are still low."

Captain Hoag: "John, bring 'er up."

A lightning flash occurred off to the left. Then, instantly, a blinding flash, an overwhelming shudder - the aircraft metal structure and body seemed to vibrate under a massive pressure and energy wave.

Hoag: "We've lost number 1! Push it all the way forward!"

Pearson: "Okay"

Hoag: "All the way forward - all the way forward - oh."

The plane hit the earth with a great screech, scrape, a shower of sparks, and a grinding of metal. It then rose again, lumbering and awry, as if struggling to be airborne - struggling - then it smashed again to the ground. The tail buckled. Flames broke out.

Fifty-six people were killed - including the crew. A number of people were injured.

HYPOTHESIS NO. 1: The piercing lightning strike to the left-hand engine caused a large atmospheric pressure wave. This wave traveled through the engine intake into the main engine chamber, snuffing out the flame, and thus the engine power.

HYPOTHESIS NO. 2: The lightning strike to the engine established a large electrical current flow in the engine structure and cowling. Electrical circuits connected to the structure experienced voltage transients causing valve malfunction and leading to an engine shutdown.

This case is dramatic. It is awesome. It commands attention. We recognize that we must protect against this type of event, model it, and develop reiterative computations and tests to uncover the boundaries of transient energies invading important electrical circuits.

This case is given to illustrate the contrast between a very visible and threatening electrical upset or damage phenomenon and the usual run of invisible Electromagnetic Interference (EMI) unfamiliar to most airline passengers. Normal electromagnetic interference environmental problems ordinarily have not carried with them the drama of the above case. Aircraft have been constructed with controls and electrical apparatus having EMI problems but not having any influence on safety.

Knowledge of and protection against induced noise voltages are necessary today. They will be even more necessary in future aircraft where vital and critical control functions are being taken over by avionics interconnected by digital data buses. These data buses that could impair safety if beset by electrical noise. We need access to knowledge of the various types of noise. There is a growing awareness of electromagnetic interference and Electromagnetic Compatibility (EMC).

### 1.1.2. Electromagnetic Compatibility

Electromagnetic interference could cause a flight delay or endanger the operation of an aircraft at 30,000 feet. Generators of electromagnetic interference for aircraft (figure 1.1-1) take on several forms:

- Transmitters of radio frequencies that mav be installed on the aircraft itself, such as High-Frequency (HF) or Very High-Frequency (VHF) communication links, or high-energy sources located on the ground such as our everyday frequency modulated (FM) radio or HF-VHF-UHF broadcast stations.
- The aircraft power line 400-Hz electric and magnetic fields.
- The computer and avionics microprocessor timing and control clock signal circuits that generate radio frequencies of one MHz or higher.
- The aircraft power switching regulators which are used to convert from one level of power to another.

Electrical switching transients sparked by the turn on and off of aircraft lights, fans, and engines or by the operation of control surfaces, ailerons, slats, and flaps.

Electrostatic discharges including lightning.

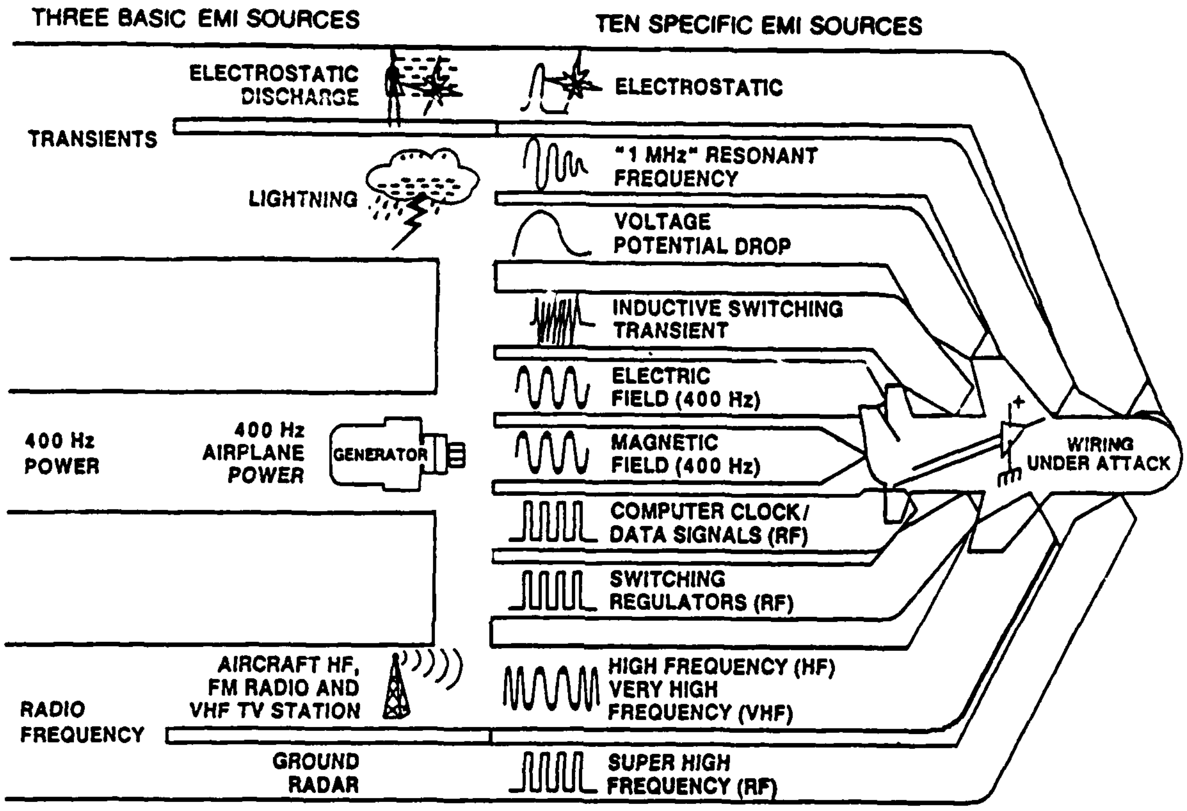


FIGURE 1.1-1. REPRESENTATIVE EMI SOURCES

These transients and electromagnetic waves may transfer into wiring and cause "electromagnetic interference" to microcircuits inside electrical equipment and avionics. This interference could result in a trifling disorder in a flight deck display or, more seriously, an engine shutdown.

The conductive paths of electrical wiring provide an avenue to usher electromagnetic interference directly to airplane avionics and signal inputs. Eliminate wiring, and electromagnetic interference almost vanishes. Wiring is the most important factor in electromagnetic interference and electromagnetic compatibility. Of much less importance is the electromagnetic interference path through the avionic equipment metal housing or case. Wiring is the electrical interface and connection between avionic equipment. Its designated job is to transfer avionics signals, data, and information. In that function, it can often act to transfer electromagnetic interference energy to other wires in a wire bundle. It also sprays or radiates like a transmitting antenna and very efficiently receives radio frequency energy like a receiving antenna.

Recently, an experienced electromagnetic compatibility engineer, "an old hand," was asked, "What's the number one requirement for an electromagnetic compatibility design program that will rule out electromagnetic interference problems?"

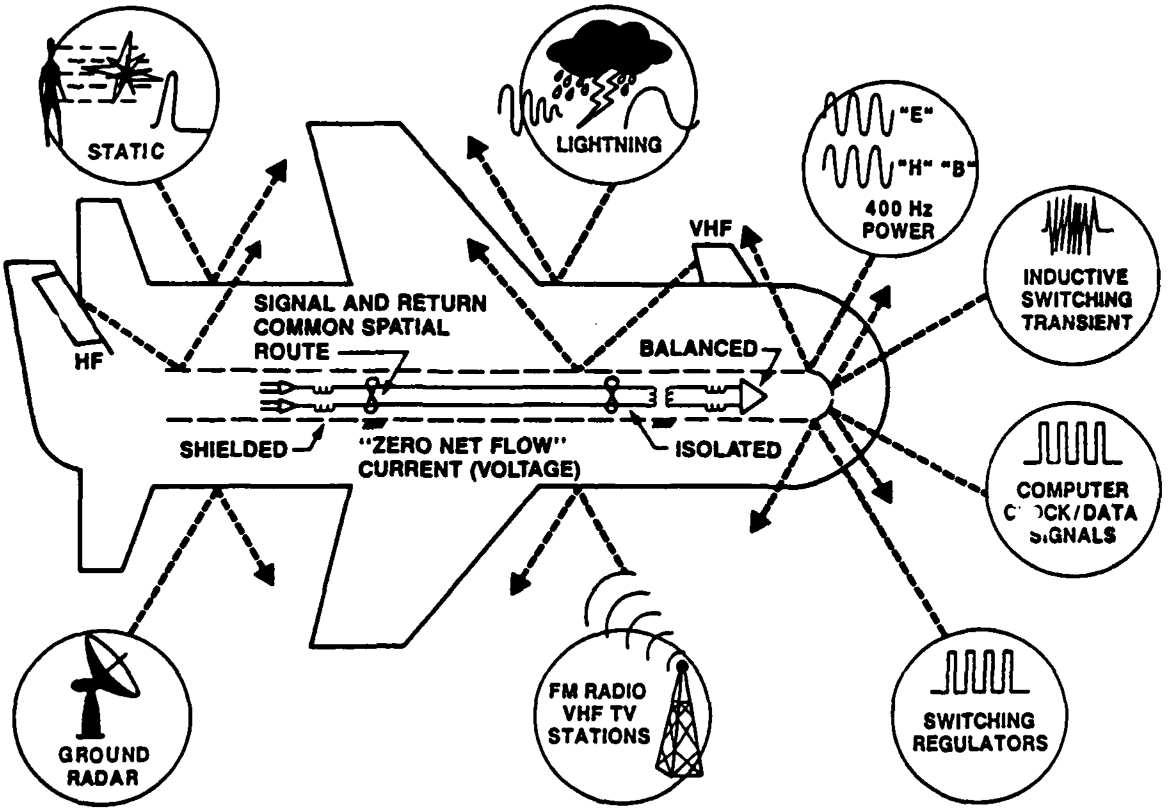

STATIC
LIGHTNING
"E"
"H" "B"
400 Hz POWER
INDUCTIVE SWITCHING TRANSIENT
VHF
HF
SIGNAL AND RETURN COMMON SPATIAL ROUTE
BALANCED
SHIELDED
"ZERO NET FLOW" CURRENT (VOLTAGE)
ISOLATED
COMPUTER C⁾ ⁾CK/DATA ъ.GNALS
GROUND RADAR
FM RADIO VHF TV STATIONS
SWITCHING REGULATORS

FIGURE 1.1-2. EMI ENVIRONMENT IN AIRCRAFT

His answer, "Zero net current flow in a shielded, balanced, isolated circuit." In other words, always route the signal wire and return or the power wire and its return together using twisted pair, coax, or shielded pair, which means that aircraft basic structure is not used as the return path for the circuit (figure 1.1-2). This will almost eliminate the three electromagnetic interference avenues of entry: common mode impedance paths, magnetic field coupling, and electric field coupling. (Common mode impedance conditions exist when two circuits share a portion of the same electrical path.)

So, that's it: use a return wire and use a shield for each circuit.

Without good shielding, the results are predictable. Removing the shield from the circuit and separating the return from the signal wire not only destroys the efficiency of the circuit, it also opens up the circuit to intervention from stray electric and magnetic fields. These fields provide an avenue directly to the micro-processor memories, computers, and controllers that are needed for aircraft operation and for processing and control of flight deck displays and instruments. A recent estimate of airplane problems (figure 1.1-3) indicates that power line electric and magnetic field coupling (30%), radio frequency fields (20%), transients (15%), and common mode impedance paths (10%) make up a total of 75% of deficiencies. These can be largely corrected with proper wiring design. Electromagnetic interference may occur in many of the aircraft subsystems (figure 1.1-4). If uncontrolled, it appears as radio tones, static, or 400-Hz hum on the passenger entertainment systems. It can show up as flight deck display distortion or illegibility, impaired data transmittals, computer memory loss, and may even result in suspension of equipment operation. Radio frequencies are becoming more of a concern. Today, the predominant radio frequency fields that impair avionic equipment operation fall into the HF-VHF radio frequency spectrum (figure 1.1-5). In future aircraft, the range may vary. (See section 10, Bibliography, ECAC Study.) Electromagnetic compatibility requirements encompass almost every subsystem on an aircraft.

The field of electromagnetic compatibility is not only a discipline in itself, it is also the cornerstone in the proper application of other engineering technologies. Good engineering design techniques employed in the areas of avionics, wiring and cabling, electrical bonding and grounding, lightning protection, and others, go a long way in achieving electromagnetic compatibility. Electromagnetic fields are produced by the generation, transmission, and utilization of electrical energy. Stray electromagnetic energy is generally not desired, and quite often interferes with the operation of electrical/electronic equipment, hence, the name electromagnetic interference. Control specifications for electromagnetic interference generation and electromagnetic interference susceptibility are required to achieve electromagnetic compatibility. With proper wiring, shielding, and application of voltage limiters in a good electromagnetic compatibility design, there is increased confidence in equipment operation which converts directly to the bottom line of on-time dispatch for the airlines and their passengers.

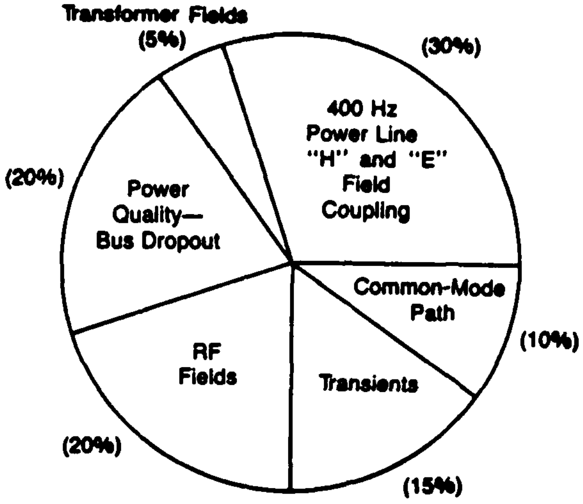


FIGURE 1.1-3. PERCENT TROUBLESHOOTING-A/C

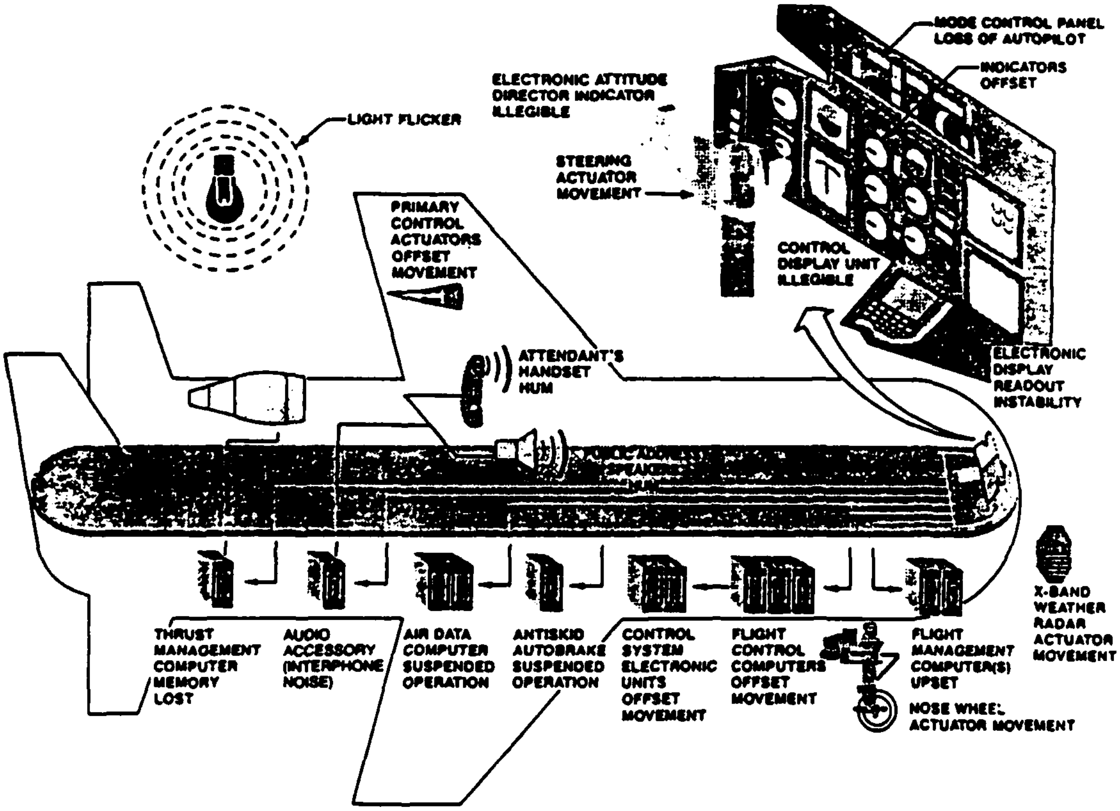


FIGURE 1.1-4. ELECTROMAGNETIC INTERFERENCE EFFECTS

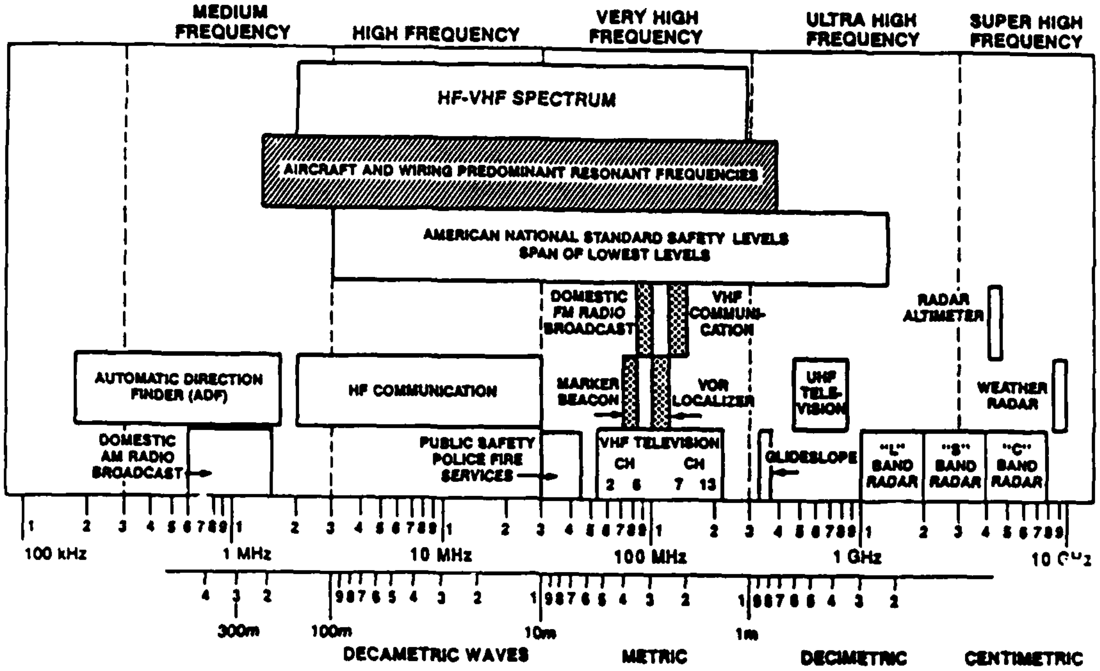


FIGURE 1.1-5. RADIO FREQUENCY RANGE

The steps to reach electromagnetic compatibility in an airline are basically threefold: (1) procure equipment and wiring according to EMC specifications, (2) package the equipment and wiring in the aircraft to obtain protection from structure, and (3) measure and test the equipment and wiring for all aspects of EMI during the program to guarantee verification and validation of EMC (see section 7, Verification and Validation).

EMC specifications for the commercial airplane are covered by Federal Aviation Regulations (FAR) and are specified in terms of system operation. FAR, Part 25.1353, Paragraph A, covers electrical equipment: "Electrical equipment controls and wiring must be installed so that operation of any one unit or system of units will not adversely affect the simultaneous operation of any other electrical unit or system essential to safe operation."

FAR, Part 25.1431, Paragraph C, covers electronic equipment: "Radio and electronic equipment, controls and wiring must be installed so that operation of any one unit or system of units will not adversely affect the simultaneous operation of any other radio or electronic unit or system of units, required by this chapter."

Environmental and emission control specifications for electronic equipment intended for installation in aircraft are documented in the current revision of Radio Technical Commission for Aeronautics (RTCA) Environmental Specification DO-160. (See sections 5 and 9.)

## 1.2. Electromagnetic Compatibility Priorities

### 1.2.1. Responsibilities and Policies

A new airplane presents a challenge of equipment location, packaging, assessment of environment, and resolution of new technology problems. The airframe manufacturer takes on the responsibility in the electromagnetic compatibility design to outline the operational-temporal-spatial anatomy of the airplane early in the conceptual stage. It is a difficult and extensive task. (See sections 4.2 and 4.3.)

Equipment location, wiring, transmitters, receivers, 400-Hz power, lightning diversion, and static dissipation are all familiar items to be pursued, tracked down, identified, and recorded. They absorb many labor hours.

Even with the rapid advance of technology, many components, characteristics, and parameters on a new airplane do not change. The electromagnetic compatibility engineer has a responsibility to know the off-the-shelf equipment. A productive policy is to seek out and rely on existing specifications and designs to the greatest extent possible, thereby sidestepping duplication of effort in analysis, scheduling, and testing. EMI test levels documented in the current issue of the RTCA Document DO-160, in many instances, represent today's environment. (They do not take into account the effects of new composite structures.) The test levels have been developed over the years. Airframe manufacturers and subcontractors can take good advantage of existing specifications and test data.

So, the first priority of the airframe manufacturer is to take on the task of defining the electromagnetic compatibility anatomy - existing equipment, new equipment, new environment, and locations.

Location often sets the electromagnetic compatibility requirements for avionics. Electronics or lack of it influences design requirements for equipment. (See section 6.)

The first priority of the avionics supplier or subcontractor (including in-house suppliers) is to know the electromagnetic interference environment and then identify, design, and protect each power input and signal input to guarantee that the equipment will operate within performance standards in that environment. The designer must shoulder the responsibility of knowing the interface wiring. Often the designer is concerned with operational requirements and must make a special effort to recognize the noise requirements. DO-160 is the basic industry standard. (See section 3.4.2 and section 9.)

The airframe manufacturer deals with new materials and properties, wiring, electrical bonding, shielding effectiveness, and definition of environment.

The avionics supplier deals with input/output circuit protection, internal grounding, circuit card layout, and interface wiring. The supplier must observe the board-level noise thresholds in a real-time, interactive setting to ensure no "state changes" and to ensure adequate containment of electromagnetic interference at the box level. The equipment engineer designs devices to be tolerant to magnetic fields from 400-Hz power (400-mV induced), 400-Hz electric field (up to 1,000V induced in test), radio frequencies (1V induced), transients from coils and lightning (600V), and electrostatic discharge (10,000V or higher). Future aircraft having critical fly-by-wire systems may require higher levels, especially for radio frequency fields. The designer must also install filters to control and contain emissions from the oscillator and switching regulator clock and harmonic radio frequencies. Interface wiring must be designed, agreed upon, and documented in an interface control drawing, otherwise hardware would require multiple electromagnetic interference designs.

Along with the size of a new program and the extent of its new technology, three pivotal factors influence the level of effort and are sine qua non to success: (1) management support, (2) the electromagnetic compatibility engineer's product experience, and (3) the electromagnetic compatibility experience of other participating engineers on the program. Management support means setting the priority for early resolution of requirements before formal document release of vendor technical specifications and statements of work. Product experience means minimum duplication and maximum productive effort. Experienced participating engineers means satisfactory coverage of subcontractor requirements, and good electrical bonding and wiring practices.

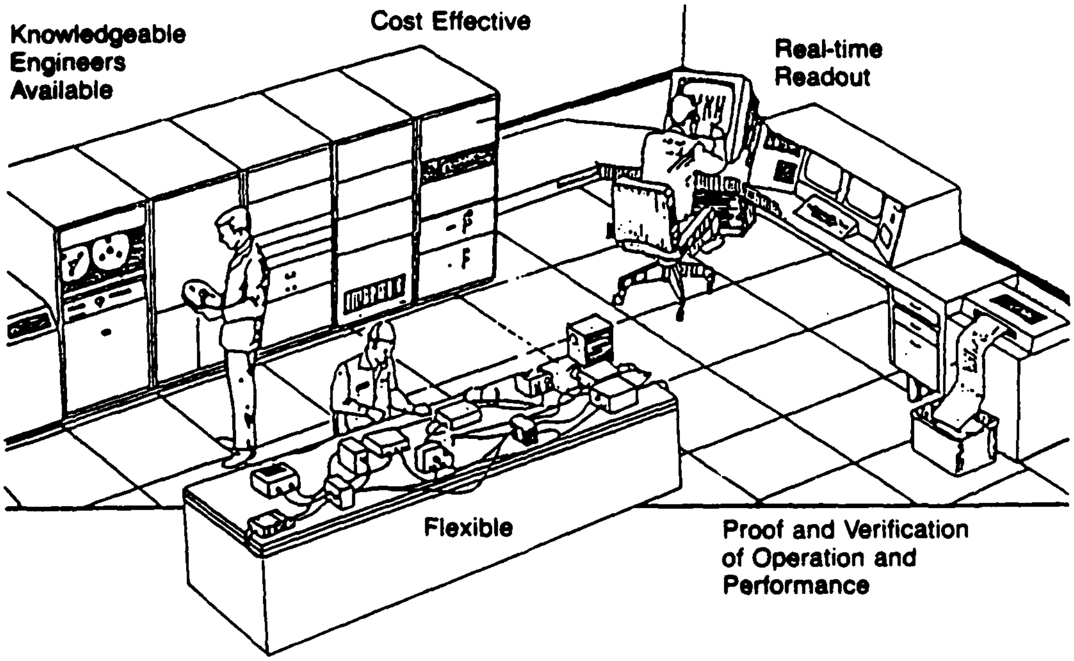

Knowledgeable Engineers Available
Cost Effective
Real-time Readout
Flexible
Proof and Verification of Operation and Performance

FIGURE 1.2-1. COST-EFFECTIVE SUBSYSTEM TESTING

On a recent airplane development program, extensive subsystem testing was performed on engineering models and production models with these three recognized benefits: (1) proof and verification of equipment performance, (2) good diagnostic testing, and (3) knowledge of equipment operation. Diagnostic/trouble-shooting tests can be run in cooperation with the subcontractor. Subsystem testing is becoming a key element in a successful program (figure 1.2-1). (See section 7.)

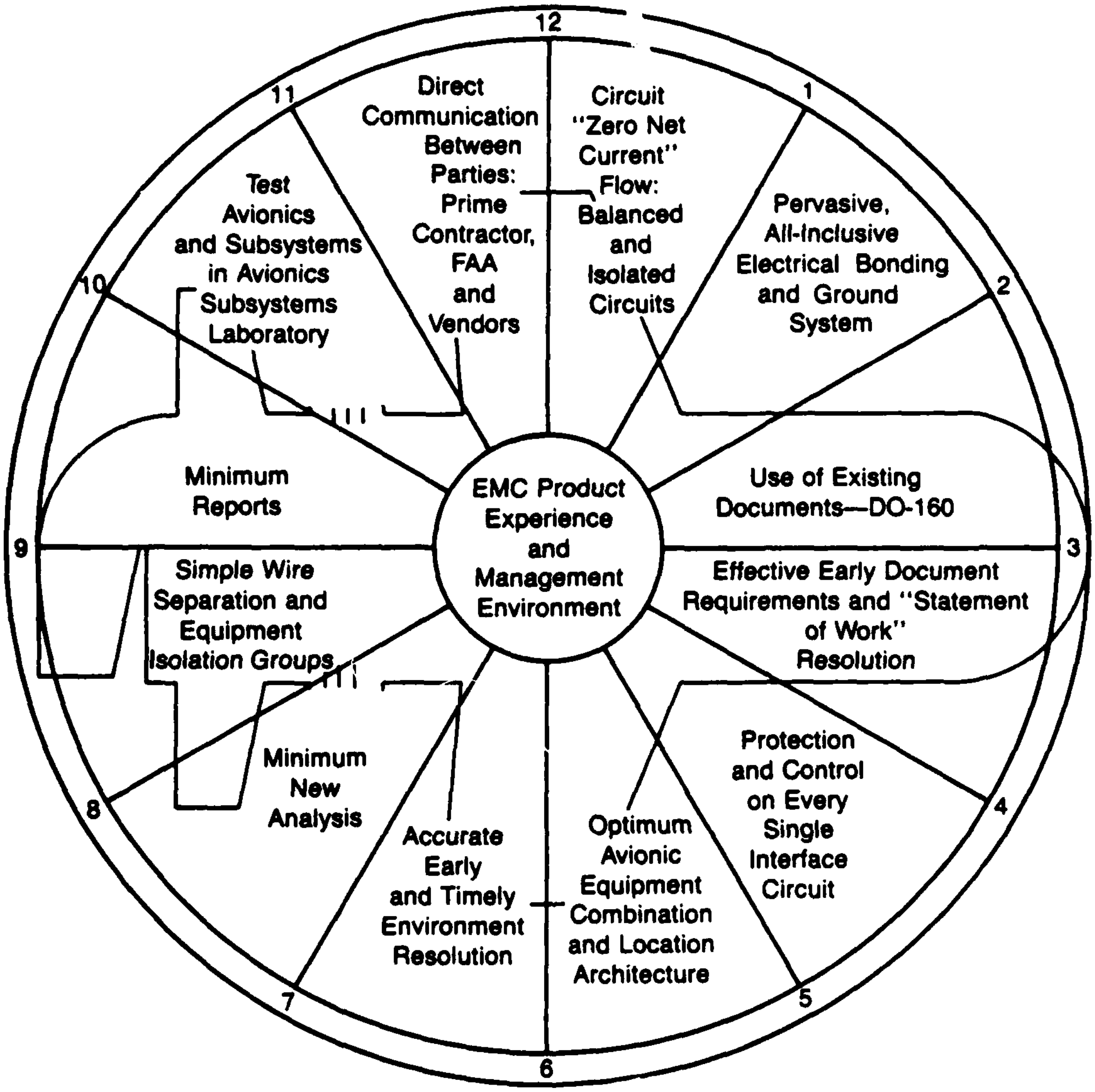

12
1
2
3
4
5
6
7
8
9
10
11
EMC Product Experience and Management Environment
Direct Communication Between Parties: Prime Contractor, FAA and Vendors
Circuit "Zero Net Current" Flow: Balanced and Isolated Circuits
Pervasive, All-Inclusive Electrical Bonding and Ground System
Use of Existing Documents—DO-160
Effective Early Document Requirements and "Statement of Work" Resolution
Protection and Control on Every Single Interface Circuit
Optimum Avionic Equipment Combination and Location Architecture
Accurate Early and Timely Environment Resolution
Minimum New Analysis
Simple Wire Separation and Equipment Isolation Groups
Minimum Reports
Test Avionics and Subsystems in Avionics Subsystems Laboratory

FIGURE 1.2-2. KEY EMC FACILITATORS

Entering into a new program incurs a commitment effort (figure 1.2-2), a commitment sized by the new technology and environment, and a commitment that dissipates with the settling of each subcontractor requirement, each design, each test, and each verification. Early adoption and documentation of known steps for successful electromagnetic compatibility are established on these baseline technical priorities: (1) zero net current flow in a balanced, isolated, shielded circuit, (2) total, all-inclusive electrical bonding of every structure and every detail (including conductive paint on external dielectric surfaces), and (3) optimum avionic equipment in-line design and location making maximum use of structural shielding.

### 1.2.2. Documentation

To provide a foundation, baseline, reference, and continuity, there are these key documents: system level specification ,possibly a paragraph or two), electromagnetic compatibility plan (may be brief), electromagnetic compatibility requirements (extensive and detailed), procurement specifications (with statements of work), interface identification, equipment test (procedure and report), and airplane test (procedure and report). (See sections 5 and 6.)

Procurement specifications must be finalized before contract formal approval.

The fact that minimum documentation leads to a more productive program is as fundamental as the fact that there are certain program top documents that must be instituted to define scope and intent and to reference industry specifications. The documentation of many of the tasks, analyses, and tests on a program can be covered by brief individual memorandums or reports. Some programs issue design notes, a practice that is an efficient method of recording and disseminating design requirements, rationale, and information.

## 1.3. How to Use This Document

The purpose of this Aircraft Electromagnetic Compatibility document is to digest, unify, highlight, and give perspective to the substantive aspects of electromagnetic compatibility applied to a commercial transport aircraft. The material in this document is not new. A very important resource to the electromagnetic compatibility engineer is the electromagnetic compatibility knowledge of other individuals associated with a program. Beliefs exist that graphite-epoxy is an insulator; that box-to-box radiation is important (it is the interface wiring that is the key to EMC); that shield tie (pigtail) length is not critical; that every single interface line does not need to be analyzed for protection and emission control; that ground planes are not required; that single-point grounding is always good (it is good for power, but not good for digital circuitry); and that extensive verification procedures can be ignored and are not essential.

The 1970s and 1980s have seen a striking rise in the quality and extent of EMC/EMI design engineering knowledge that has important consequences for EMC. This document attempts to collect and apply that information to the airplane. Derivations and fundamentals of EMC are not elucidated. This document is limited in that sense. Reference can be made to the bibliography for some excellent articles.

EMC information not found herein:

- Fundamentals or basics of EMC.

- Formulas, models, derivations.
- Antenna-to-antenna coupling.
- Power system quality.
- Lightning.

EMC information included:

- Aircraft-applied EMC.
- Architecture, equipment layout.
- Dominant EMI environments.
- Circuit susceptibilities.
- Bonding, grounding, shielding.
- Wiring design.
- Verification, validation.

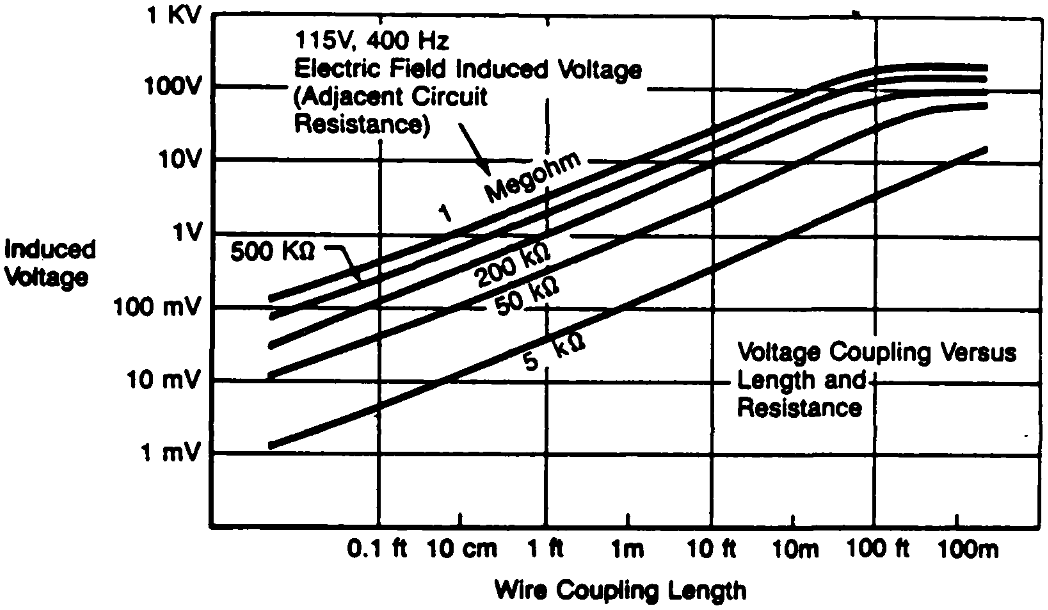


FIGURE 1.3-1. REPRESENTATIVE "E" FIELD COUPLING

It is recommended that this document be read thoroughly before concentrating on specific sections. This document is not a design document or a "design cookbook." In no way can it replace specific analysis and design effort. It is a set of guidelines to outline and scope deficiencies and qualities in present day aircraft that may aid in the approach to future designs. The information and data is illustrative and advisory to provide definition and make comparisons of parametric properties and behavior, and it is not for use or adaptation to specific designs. For example, figure 1.3-1 maps the expected voltages induced in a single aircraft wire circuit (having resistive loads) from an adjacent 115V, 400-Hz power wire where both have their returns in aircraft structure. This figure illustrates the significance of length of coupling and resistive loads and gives a rough estimate of amplitudes. But there are other interacting parameters that might be considered; ergo, each circuit type in the aircraft must be evaluated separately.

Much emphasis on wiring design exists in this document. The soul of EMC is a balanced, isolated, shielded interface circuit. It closes the door on EMI. It rejects transients, radio frequencies, and 400-Hz fields. It is practically impervious to conductive, inductive, and capacitive transfer of energy.

Linearity rises as one of the elegant attributes of electromagnetics, giving simplicity to variations in the electromagnetic dependent and independent parameters: length, height, resistance, voltage, time, over much of their range. These parameters often vary on a 1:1 ratio (20 dB per decade) or an exponential ratio, possibly 40 dB per decade. The linear relationship breaks down or changes at corner frequencies, 3 dB points, and resonant nodes where the dominance of electrical parameters make a transition from one to the other.

Ratios and the decibel relationship will be used throughout. The decibel, abbreviated dB, is a unit expressing the ratio between two amounts of power, $P_1$ and $P_2$, existing at two points. By definition, the number of dB equals 10 log to the base 10 ($P_1$ is divided by $P_2$). For special cases where $P_2$ equals 1 mW or 1W, the dB ratio is defined as "dBm" or "dBW." For power, a factor of 10 equals 10 dB. Since power P equals $V^2$ divided by R, or $I^2$ times R, decibels can be used to express voltage and current ratios where the voltages and currents are measured at places having identical impedances. By definition, dB equals 20 log of ($V_1$ divided by $V_2$), and dB equals 20 log ($I_1$ divided by $I_2$). For convenience, $V_2$ or $I_2$ are often chosen as 1 $\mu$V and 1 $\mu$A, and the dB ratio defined as dB above a microvolt or dB above a microamp. Also for convenience, these ratios are more often used whether or not they are referenced to identical impedances. A factor of 10 equals 20 dB. Memorize these voltage-current ratios: 6 dB = 2X 10 dB = 3X, 12 dB = 4, 20 dB = 10, 40 dB = 100, and 60 dB = 1000.

# 2. AIRPLANE AVIONICS AND CRITICALITIES

## 2.1. Existing Systems

The well-known hallmarks of a commercial trai 'port aircraft (figure 2.1-1) are: one-hundred and fifty paying passengers or more, flight attendants, airline competition, scheduled dispatch, fixed cost, aisles, lavatories, galleys, and video entertainment.

The necessary control of capital cost and running expenses, the need for quick and easy equipment maintenance, and the desire for on-time dispatch: these goals urge the airframe manufacturer to focus on a well-designed, well-planned electrical architecture, including electromagnetic compatibility. Standardized avionic Line Replaceable Units (LRU) are motivation for low cost and competition among subcontractors (figure 2.1-2). Cost, airworthiness, and safety are the critical drivers for avionics.

Most passengers are unaware of the safety built into the interface wiring and electrical/electronic systems (figure 2.1-3). Passenger and crew safety, with regard to protection from hazards of high voltages, has been guaranteed historically by the ubiquitous aluminum housings, spars, supports, and structure. The high-quality structural aluminum grounding paths are inherently the electrical return or an electrical reference for digital signals, shield ties, motor power current, and fault currents (figure 2.1-4). This structure bypasses the need for separately installed wires or buses to fulfill those functions (figure 2.1-5). Also enhancing the electrical sinking and conducting properties of structure are the extensive air-conditioning, water, and hydraulic systems that form a skeleton of metallic and composite materials throughout the flight deck, cabin, cargo bay, wheel wells, and wing leading and trailing edges. Many of these shielding and sinking properties today help to contain or divert electromagnetic interference from electronic game signals, electrostatic discharge, lightning transients, and high-energy broadcast radio frequencies (figures 2.1-6 and 2.1-7).

Aluminum alloys form the wing, fuselage, and empennage structure, but these metal alloys must mate with materials like fiberglass, Kevlar, and moderately conductive materials like graphite-epoxy. The interfaces at fairings, doors, ducting, and fasteners open up possibilities of apertures and gaps. These mating surfaces must be electrically bonded so that power currents, fault currents, electrostatic charge, and lightning currents flow (figure 2.1-8).

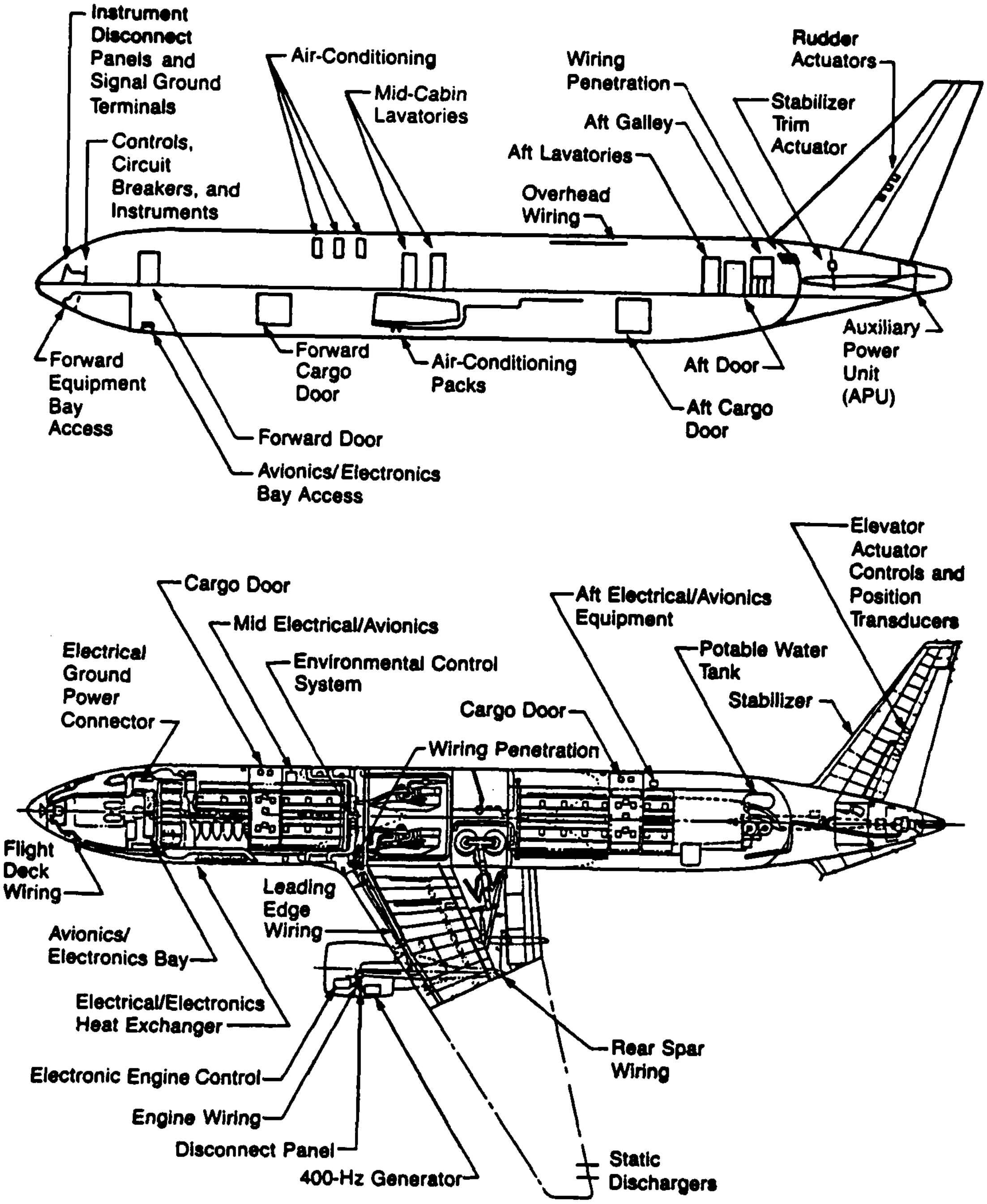

Instrument Disconnect Panels and Signal Ground Terminals
Controls, Circuit Breakers, and Instruments
Air-Conditioning
Mid-Cabin Lavatories
Wiring Penetration
Aft Galley
Aft Lavatories
Overhead Wiring
Rudder Actuators
Stabilizer Trim Actuator
Forward Equipment Bay Access
Forward Door
Avionics/Electronics Bay Access
Forward Cargo Door
Air-Conditioning Packs
Aft Door
Aft Cargo Door
Auxiliary Power Unit (APU)
Cargo Door
Mid Electrical/Avionics
Environmental Control System
Electrical Ground Power Connector
Cargo Door
Wiring Penetration
Aft Electrical/Avionics Equipment
Potable Water Tank
Stabilizer
Elevator Actuator Controls and Position Transducers
Flight Deck Wiring
Avionics/ Electronics Bay
Electrical/Electronics Heat Exchanger
Leading Edge Wiring
Electronic Engine Control
Engine Wiring
Disconnect Panel
400-Hz Generator
Rear Spar Wiring
Static Dischargers

FIGURE 2.1-1. PRESENT-DAY AIRCRAFT SYSTEMS

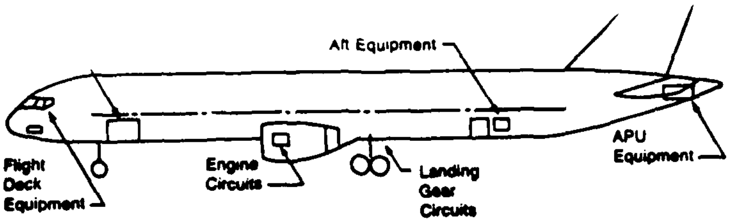


FIGURE 2.1-2. AVIONICS BAYS

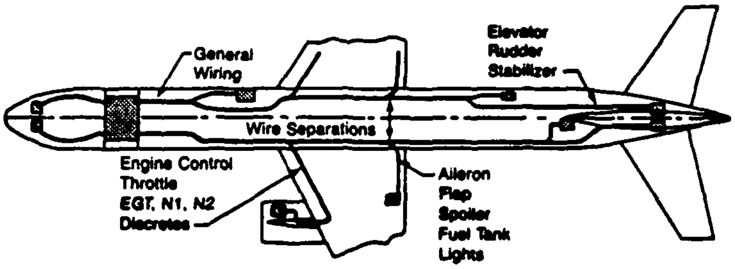

General Wiring
Elevator Rudder Stabilizer
Wire Separations
Engine Control Throttle EGT, N1, N2 Discretes
Aileron Flap Spoiler Fuel Tank Lights

FIGURE 2.1-3. WIRING

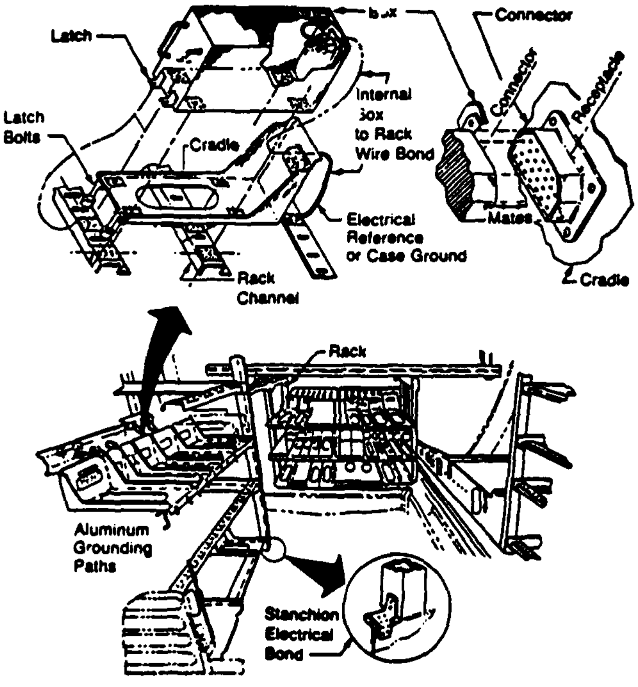


FIGURE 2.1-4. MAIN BAY ALUMINUM STRUCTURE

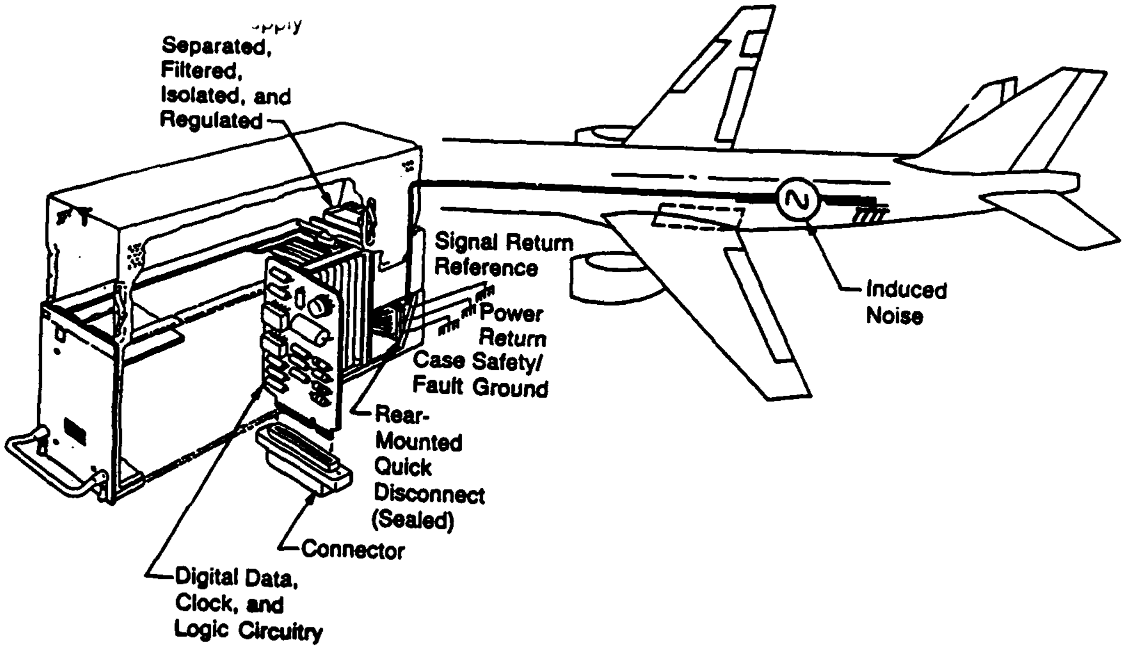


FIGURE 2.1-5. STRUCTURE RETURN

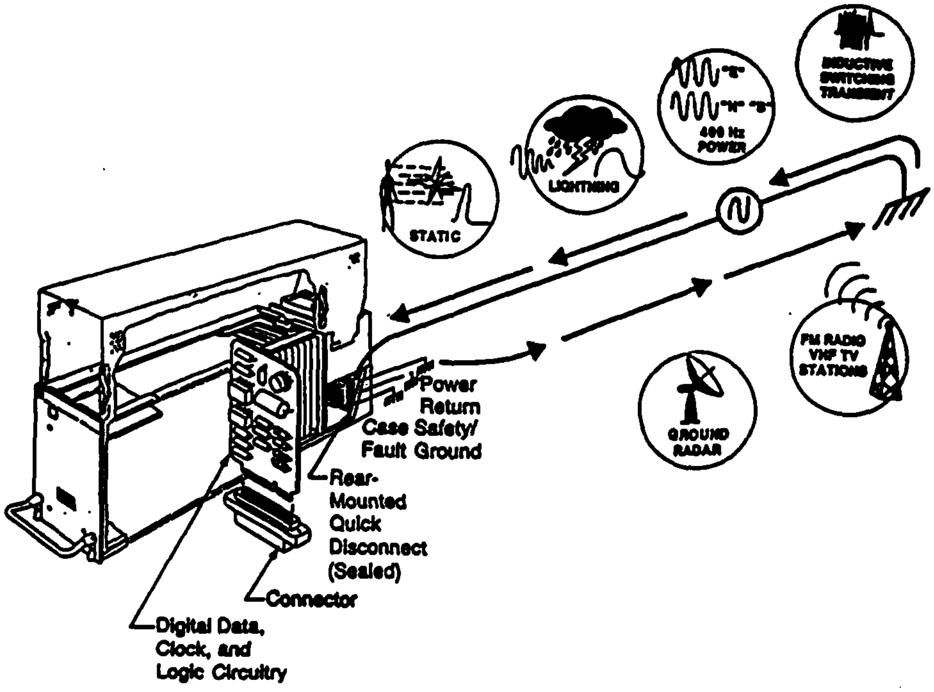


FIGURE 2.1-6. INDUCED NOISE

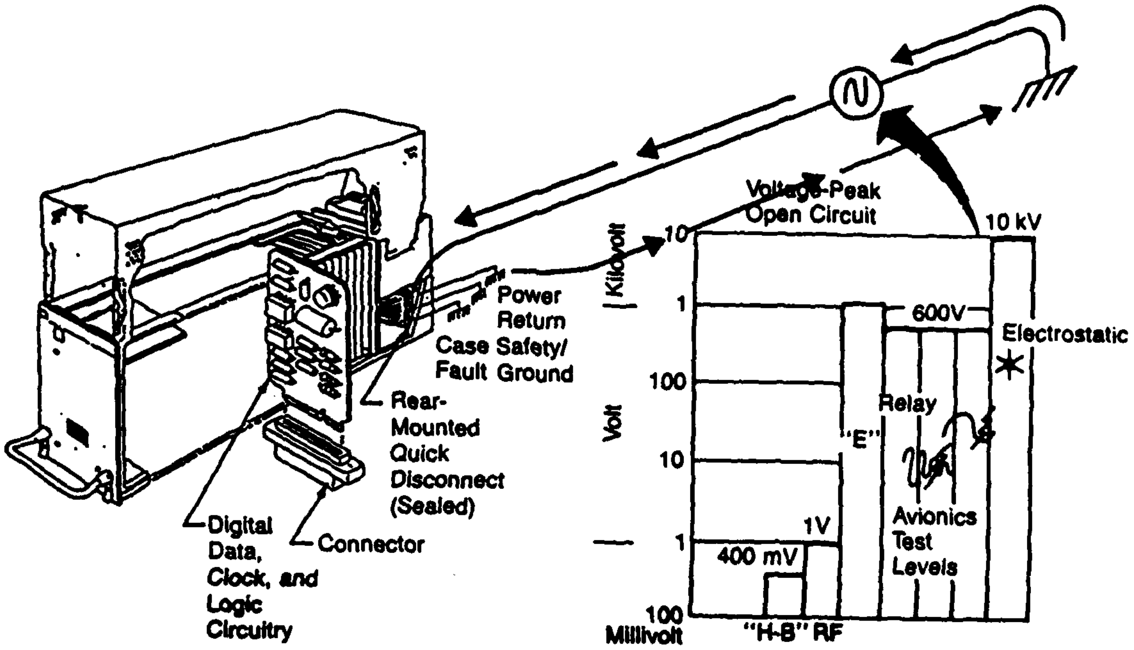


FIGURE 2.1-7. NOISE VOLTAGES

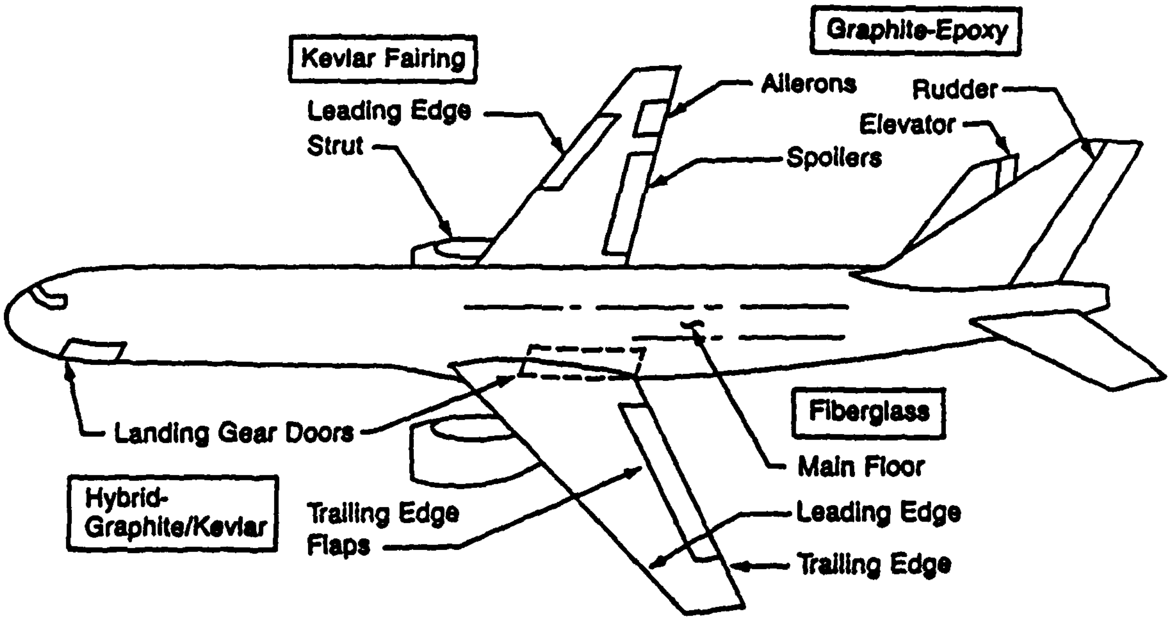


FIGURE 2.1-8. NONMETALLIC INTERFACES

With each new program, we build on the safety and electromagnetic compatibility practices of past experience, and as the program progresses, we purchase and install units of avionic equipment which were designed, built, and tested years ago - existing equipment, "off-the-shelf" equipment. So, years of in-service experience with existing equipment are brought together with the new technology designs on the new program. We cannot overlook the fact that electromagnetic compatibility and safety standards have been well established. Hence, this document does not hold any revealing secrets or creative innovations. Many of the requirements for electromagnetic compatibility are very well known having been spawned, tried, and steadily refined over the years.

With an experienced eye on airworthiness and reliability, traditional electrical and electronic functions have been carefully shaped by the airframe manufacturer and subcontractors to provide and enhance engine instrumentation (safety), communication and navigational aids (safety and convenience), autopilot equipment (pilot workload), and aircraft utilities (safety and passenger comfort). Redundancy of avionics functions and components has become a de facto standard. Avionics equipment in today's aircraft (1986) strongly contribute to the desired levels of performance and safe flight through separation and duality (figure 2.1-9). Any one single part or unit in a fully operational and functioning aircraft is not vital and crucial to continued flight. Triple redundant flight control computers and data buses, for instance, practically guarantee continuous operation and provide a confident reliance on the automatic pilot system (figure 2.1-10). Electromagnetic compatibility is important and must be "designed in" to be cost effective or the avionic equipment will not work, but electromagnetic compatibility has not been critical to aircraft safety.

Engine monitors or sensors are becoming critical, especially on the new electronic engine controls (figure 2.1-11). Left engine circuits are separated from the right for safety. Selected circuits on each engine are separated from each other. Oil pressure transducers, engine temperature thermocouples, exhaust gas temperatures (EGT), and speed sensors (N1, N2) provide information on performance and operational boundaries and status. Knowledge of the status of hydraulics, oil, and fuel systems helps avert critical situations. Throttle lever angle position must be known, and of course, fire detection is mandatory. Electromagnetic interference must be designed out of these circuits early in any program.

Communication receivers and transmitters are the key in today's flight schedules and goals of smooth flight and fuel economy (figure 2.1-12). Noise must be at a minimum to keep from degrading receiver thresholds. Broadband noise will reduce communication range. Narrow band noise will induce unwanted tones. The flight crew does not want to hear static, 400-Hz hum, or popping, even though this electromagnetic compatibility problem may only be a nuisance.

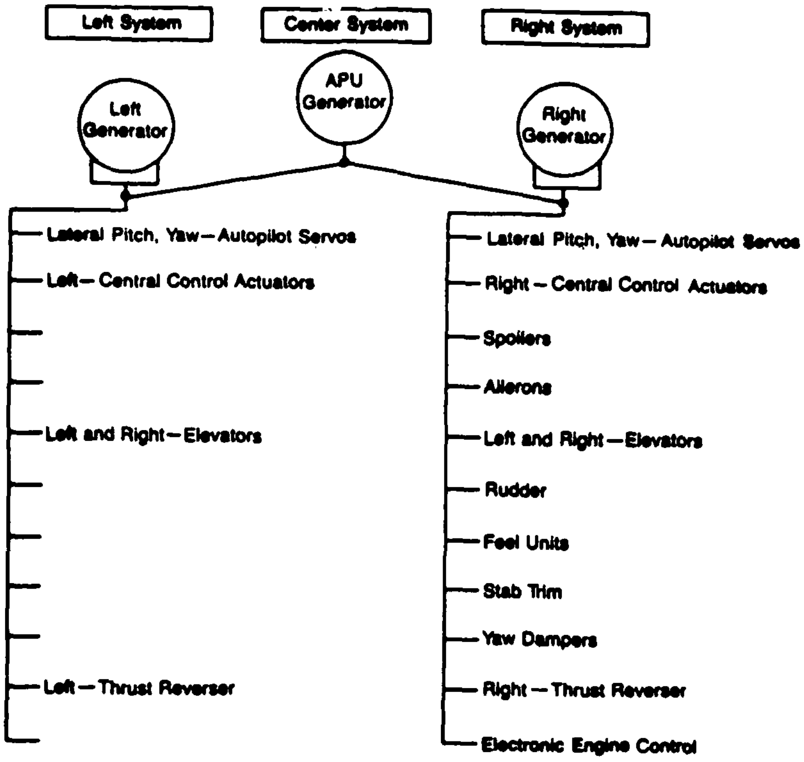


FIGURE 2.1-9. SEPARATION EXAMPLE

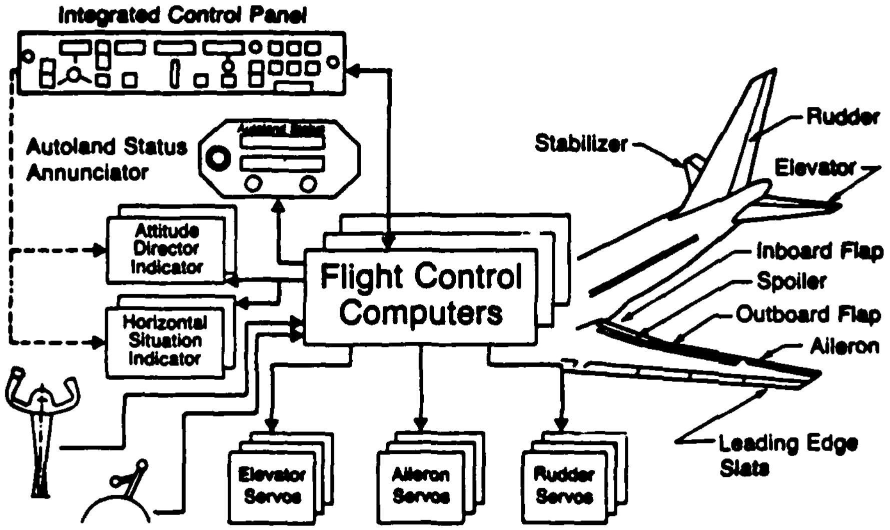


FIGURE 2.1-10. FLIGHT CONTROL AUTOPILOT REDUNDANCY

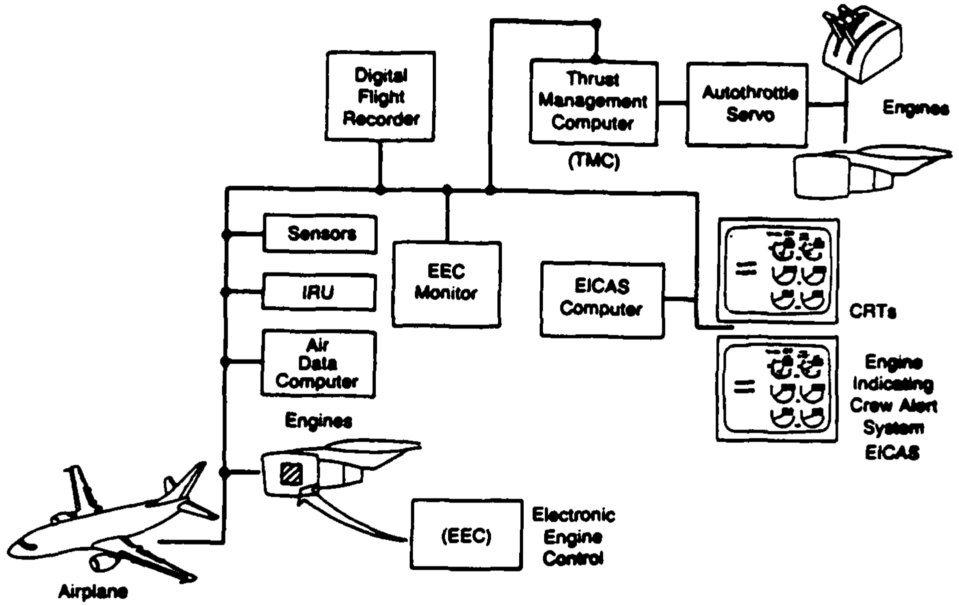


FIGURE 2.1-11. ELECTRONIC ENGINE CONTROL

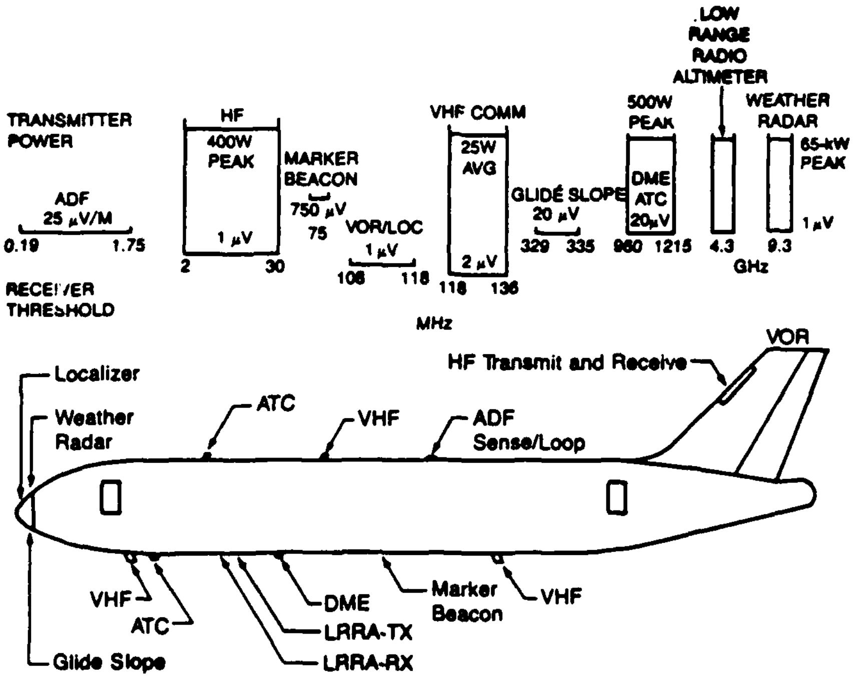


FIGURE 2.1-12. TRANSMITTERS-RECEIVERS

Automatic controls reduce pilot workload and assist in long flights and optimum flight profiles (figure 2.1-10). We still see the old-fashioned compass installed in the instrument panel on the flight deck, but the "horizontal situation indicator" is now a Cathode Ray Tube (CRT) (which, by the way, is very susceptible to 400-Hz magnetic fields) and is designated as the electronic horizontal situation indicator (EHSI). There are two EHSIs to rely on besides the old-fashioned backup compass (figure 2.1-13). Future aircraft will see flat panel displays that must be protected from radio frequencies and transients that induce "snow," "banding," "lines," or "ripple" on the screen.

Today's professional pilot "flies" the plane with the steering column having steel cable strung from the column to hydraulic actuators which then amplify the force and operate control surfaces (figure 2.1-14). The engine throttle is operated by a steel cable. A steel cable does not recognize electromagnetic interference.

Navigation equipment with ground systems that locate and track have grown more and more sophisticated, accurate, and reliable (figure 2.1-15). Specifications and requirements have been developed over the years (table 2.1-1). VHF and HF communications are used over land and sea, all along the airways, and in high-volume areas (figure 2.1-16). Communication avionic units are stand-alone components that can be individually replaced in the electronic equipment bay or on the flight deck (figure 2.1-16). Because of the excellent flexibility of unit replacement, ease of maintenance and substantially lower unit costs, there has been little or no historical incentive for large-scale integration of functions on present day airplanes (figure 2.1-17). Most equipment today is basically digital, but some is still analog (figure 2.1-18). Future aircraft will probably see almost total use of digital circuitry.

Aircraft utilities, of course, are basic to commercial transport operation. Fluorescent lights in the cabin are noisy. Pressurization controls, cooling fans, and window heaters contribute to aircraft magnetic fields. Cargo handling and windshield wiper motors, fans, and galley heaters inflict broadband noise on digital and analog circuits. Future systems may have pulse width modulated voltages that will contribute to noise.

Today's interface circuits span the systems from engine instrumentation to navigation to flight control to utilities, but electromagnetic compatibility engineers do not deal with flight systems. They deal with circuit types, and basically those types can be counted on two hands. The types can be boiled down to digital data, radio frequency signals, analog signals, discrete state changes, and 400-Hz 115V or 28V-dc power and in the future pulsed dc power.

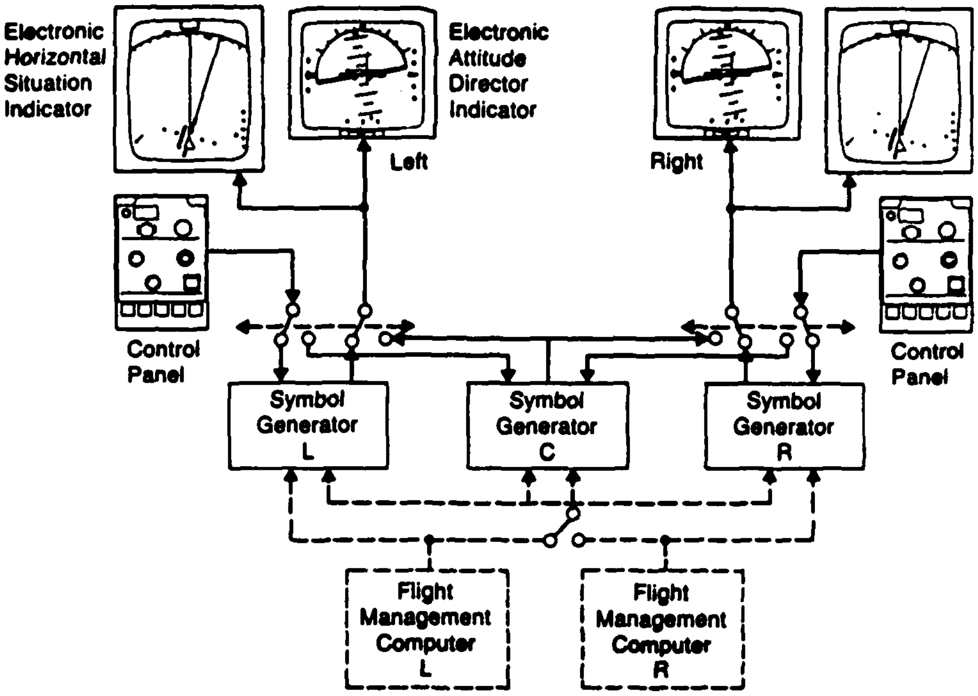

Electronic Horizontal Situation Indicator
Electronic Attitude Director Indicator
Left
Right
Control Panel
Control Panel
Symbol Generator L
Symbol Generator C
Symbol Generator R
Flight Management Computer L
Flight Management Computer R

FIGURE 2.1-13. FLIGHT INSTRUMENT SYSTEM

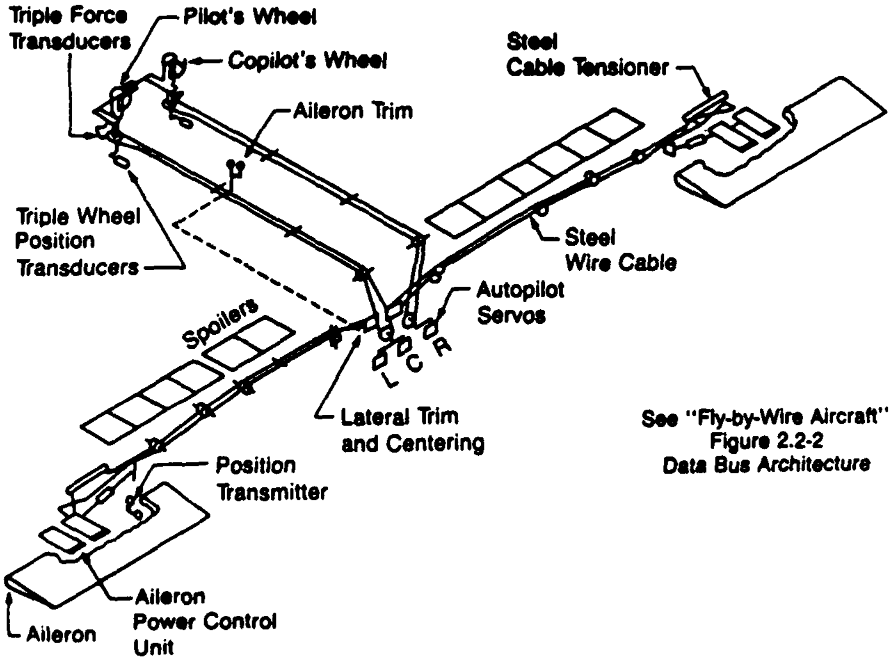


FIGURE 2.1-14. ROLL CONTROL SYSTEM

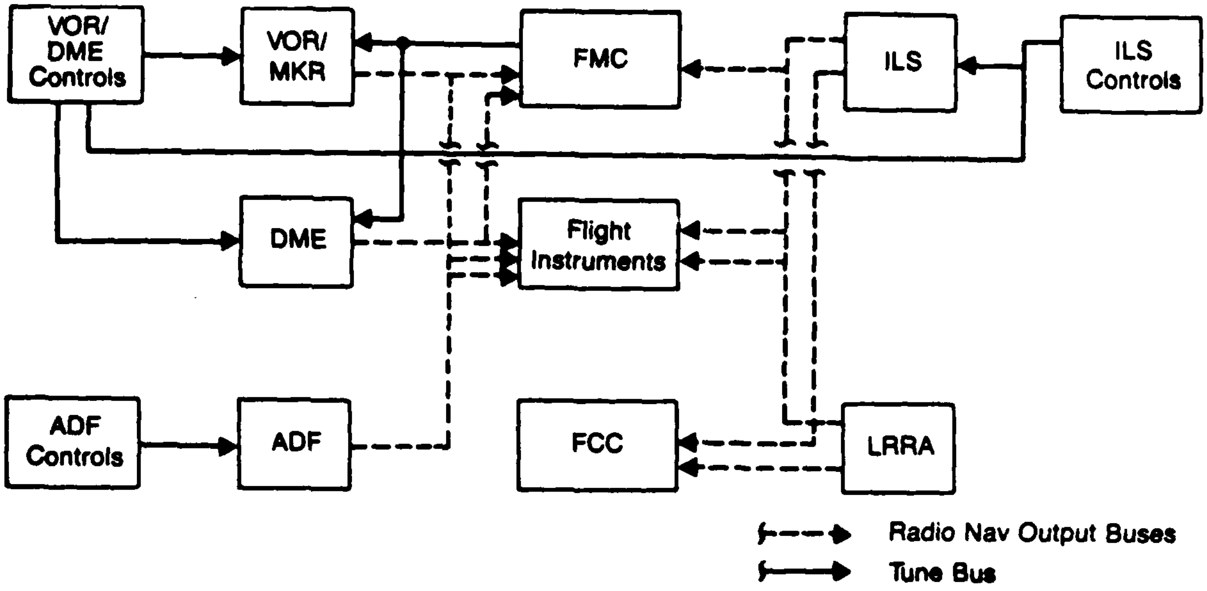


FIGURE 2.1-15. NAVIGATION

TABLE 2.1-1. NAVIGATION EQUIPMENT DOCUMENTATION

| Navigation Equipment | Federal Aviation Regulation (FAR) | Technical Standard Order (TSO) | Advisory Circular | Number Required |
|---|---|---|---|---|
| VOR | 121.349a,e | C40a | 90-45A | 2 |
| DME | 121.349c | C66a | 90-45A | 1 |
| LOC/GS | 121.349a | C34b | 120-28A | 1 |
| | | C36b | 120-29 | — |
| MB | 121.349a | C35c | — | 1 |
| ADF | 121.349b | C41b | 20-63 | 1 |
| INS/ISS | 121.355 | — | 25-4 | 2 |
| | 121, App. G | — | 121-13 | — |
| RNAV | — | — | 90-45A | — |
| Omega | — | — | 120-31 | — |

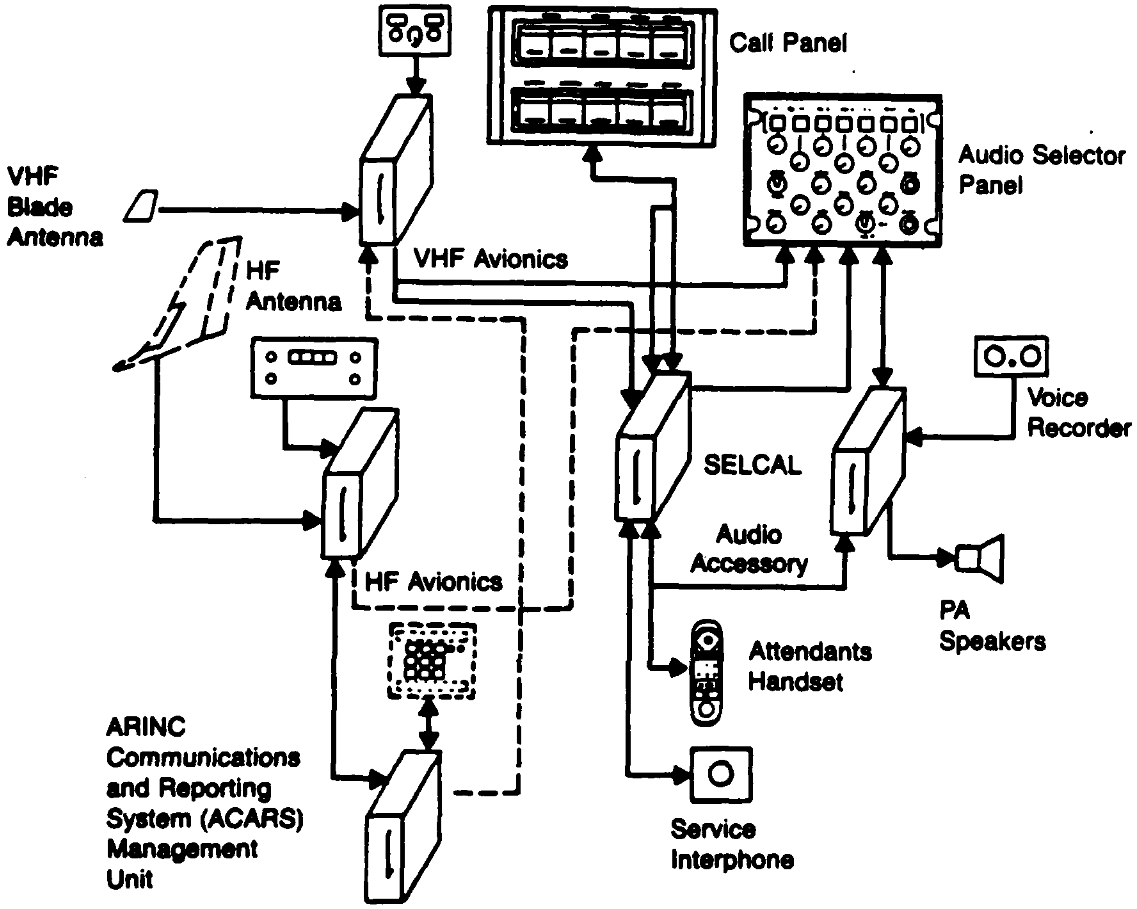


FIGURE 2.1-16. COMMUNICATION

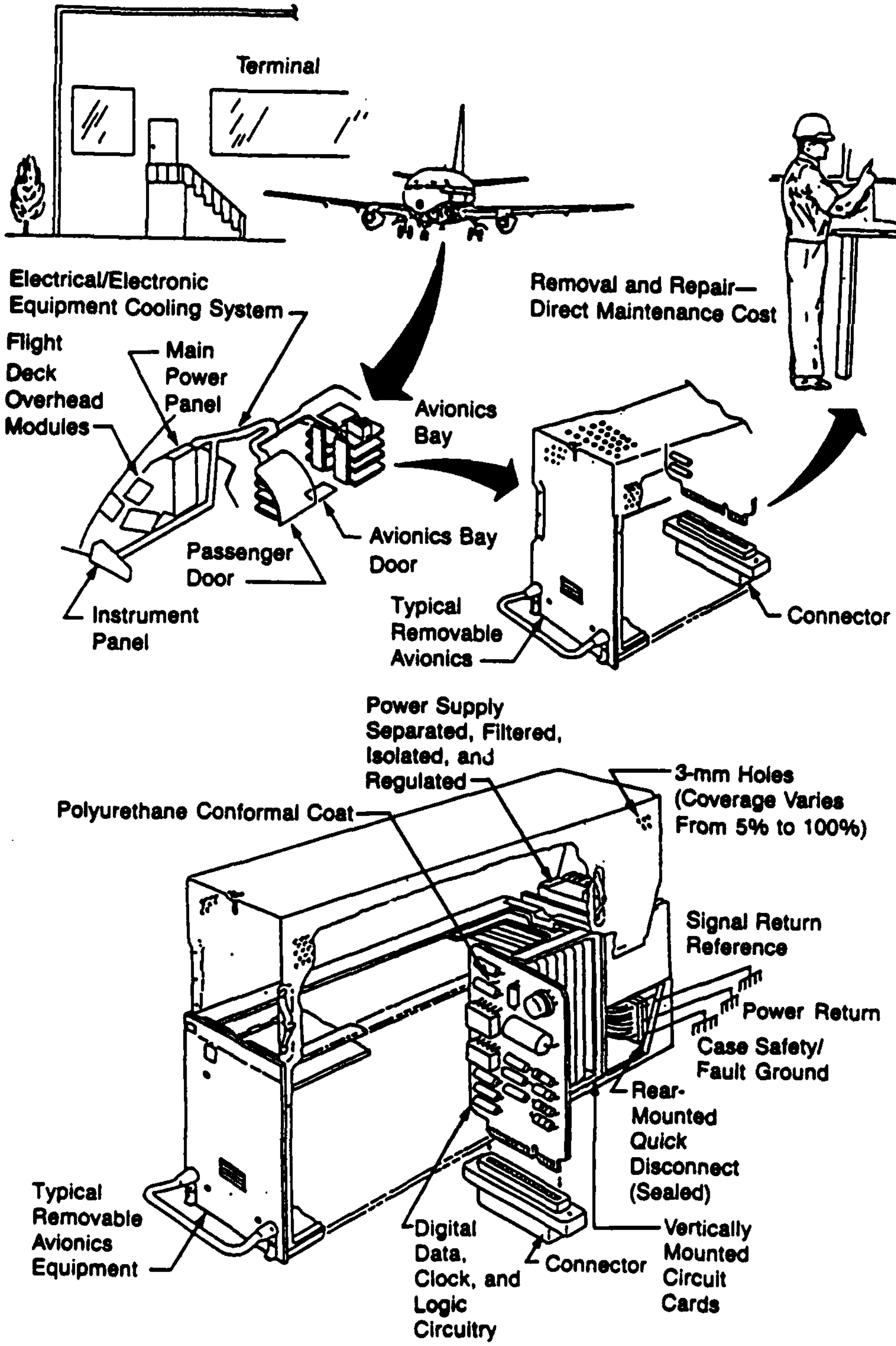

Terminal
Electrical/Electronic Equipment Cooling System
Removal and Repair— Direct Maintenance Cost
Flight Deck Overhead Modules
Main Power Panel
Avionics Bay
Passenger Door
Avionics Bay Door
Instrument Panel
Typical Removable Avionics
Connector
Power Supply Separated, Filtered, Isolated, and Regulated
3-mm Holes (Coverage Varies From 5% to 100%)
Polyurethane Conformal Coat
Signal Return Reference
Power Return
Case Safety/ Fault Ground
Rear-Mounted Quick Disconnect (Sealed)
Typical Removable Avionics Equipment
Digital Data, Clock, and Logic Circuitry
Connector
Vertically Mounted Circuit Cards

FIGURE 2.1-17. LINE REPLACEABLE UNIT

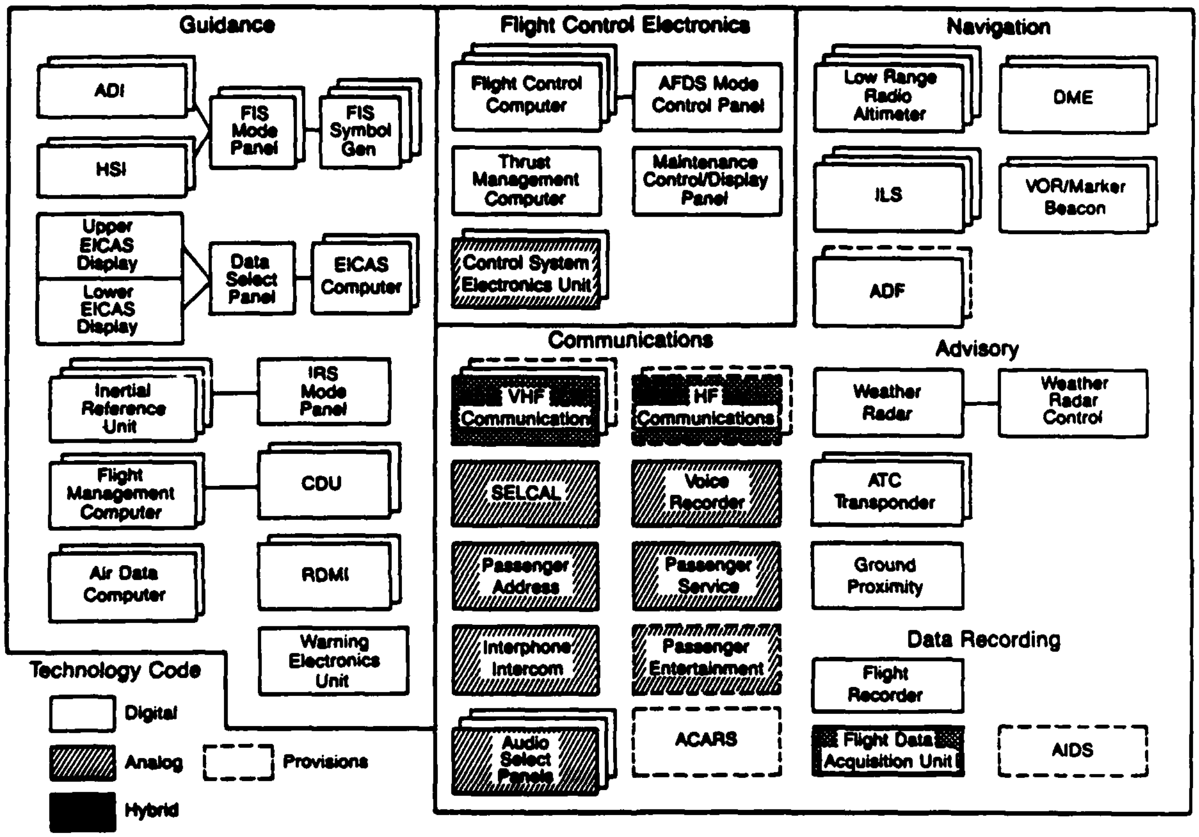


FIGURE 2.1-18. FLIGHT MANAGEMENT SYSTEMS

It one were to look at the specific types of interconnecting circuits, here are some examples of the electrical/electronic characteristics and parameters:

EXAMPLES

| CIRCUIT | | LEVEL | RATE/FREQUENCY | THRESHOLD |
|---|---|---|---|---|
| (1) | Digital data: | +5V | 12 kHz | 2.5V |
| | (ARINC 429 transmitter/receivers: information transfer, altitude, airspeed, direction, positions) | | | |
| (2) | Pulse circuits: | +50V pulse | 1 pps | mV |
| | (Fuel flow; engine speed) | | | |
| (3) | "Discrete" | +30V | Event ON/OFF | 10V |
| | (Status: Pumps, valves, relays, heaters) | | | |
| (4) | Analog | 0V to 10V | Continuous | mV |
| | (Position indicators) | | | |
| (5) | Power | 28V dc<br>115V ac | (sw. reg. 10 to 100 kHz)<br>400 Hz and harmonics | |
| | (Avionics, pumps, lights, motors, generator feeders) | | | |
| (6) | RF | Volts | Variable | $\mu$V |

The electromagnetic compatibility engineer helps to simplify and forge the layout of the equipment and routing of the wires (figure 2.1-19). He pays particular attention to radiated emission from wiring and radio frequency fields imposed on wiring (figure 2.1-20). Equipment location has been settled usually in the past by greater attention to and emphasis on temperature characteristics, size, separation, accessibility, and center of gravity factors rather than electromagnetic compatibility. And, rightly so. Wiring, wire clamps, shield ties to structure, and routing of wire-bundle installations have been shaped by the space available and structure geometry. They have been installed as an "add-on" while all the time being given the appellation of weight penalty. Conduit or metallic ground planes have not been needed. Shielding could be added any time.

We and our predecessors seldom created and documented substantive and comprehensive input/output interface circuit drawings to provide an analysis on a systematic basis of the noise sources and the major avenues of coupling. Electromagnetic interference sometimes has been most elusive and difficult to analyze, model, and predict.

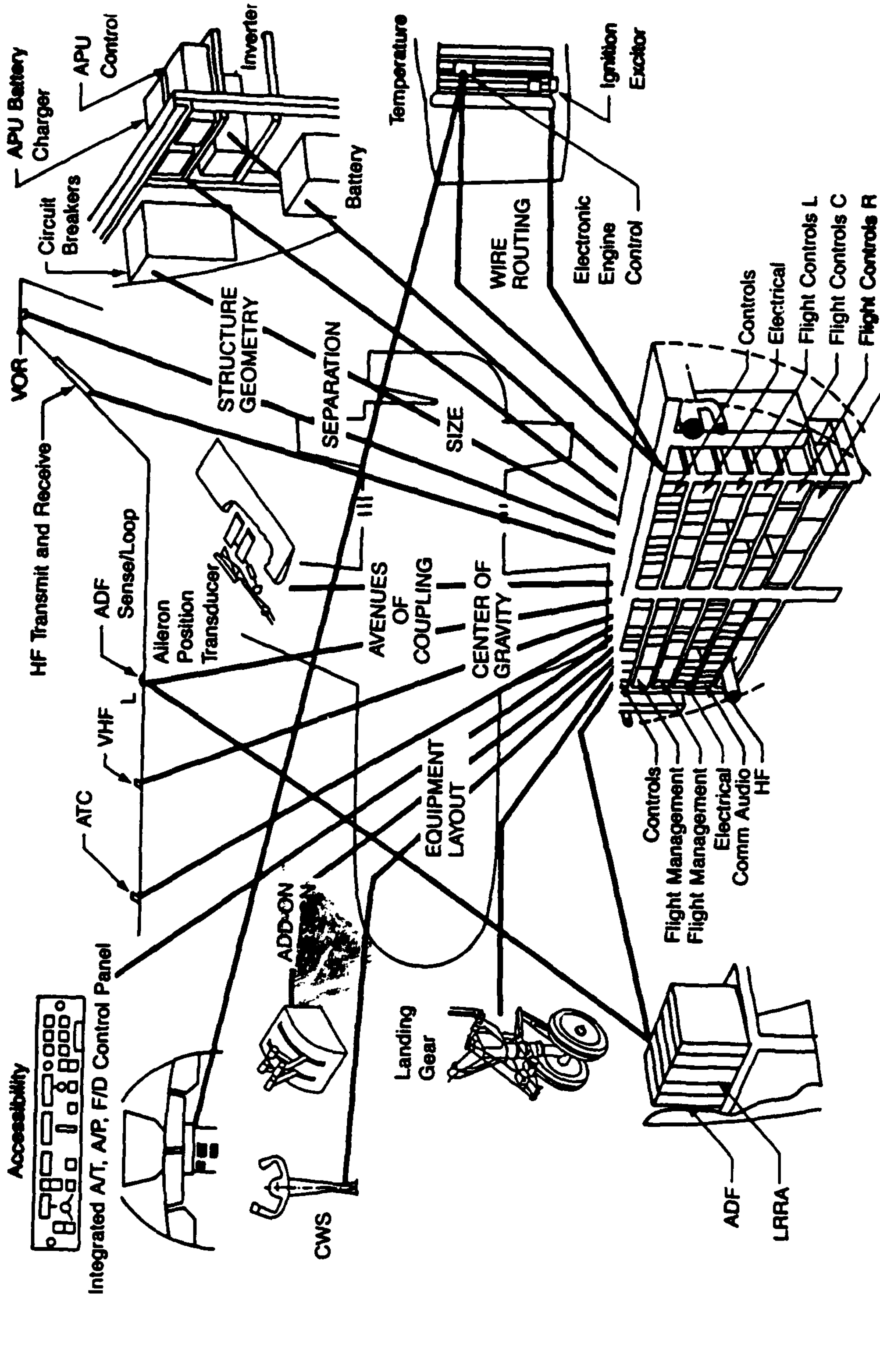


FIGURE 2.1-19. EQUIPMENT/WIRING LOCATION COMPLEXITIES

Avionic equipment units have been designed and tested to industry electromagnetic compatibility specifications and then, along with their interconnecting wiring, installed directly in the aircraft. They almost always perform properly. This method has been cost-effective and not at odds with safety. Fixes to equipment or to the airplane can sometimes be made fairly easily and inexpensively, although they are often done in a hurry and with the ever-present specter of the very expensive "retrofit."

As we look back, it is recognized that the electromagnetic compatibility effort has been reactionary, not anticipatory.

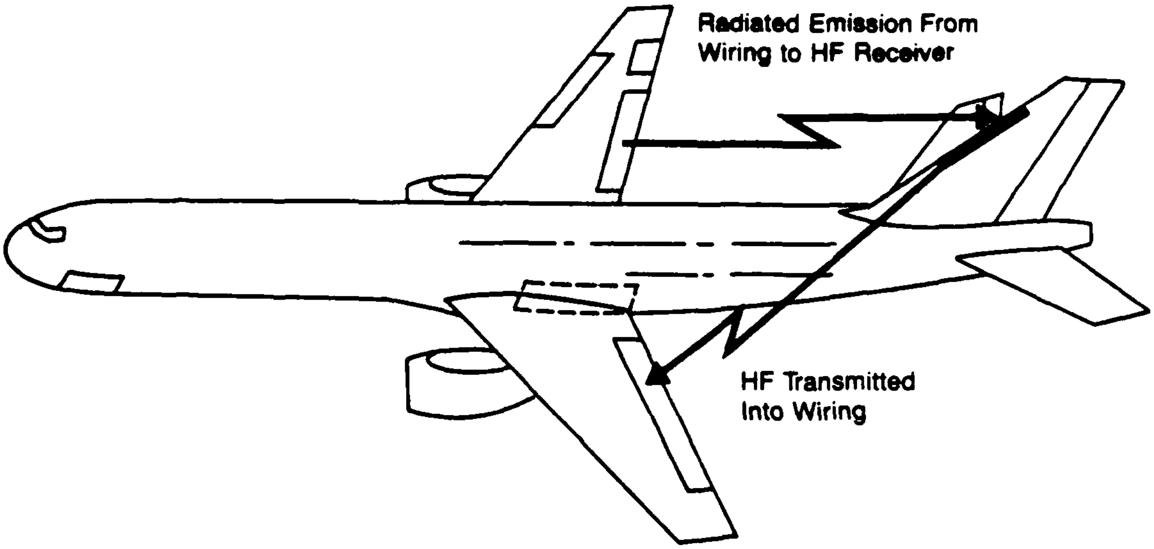


FIGURE 2.1-20. RADIATED EMISSION

## 2.2. Future Aircraft

Turn now and look ahead to a hypothetical future aircraft.

A view of a system avionic architecture might focus on the technologies of digital buses, electric actuators, and composite structural materials as having the greatest interest for the electromagnetic compatibility engineer or airworthiness specialist (figure 2.2-1). A system of communication and control designed around fly-by-wire digital data buses and electric actuators will have an impact on analysis tasks; that is, greater effort will be needed to assure absence of electromagnetic interference in the data bus and control of electromagnetic interference from the actuators and pulsed dc.

Connection of autonomous electronics through a multiple access two-way data bus will remove dependance on a centralized controlling processor (figure 2.2-2).

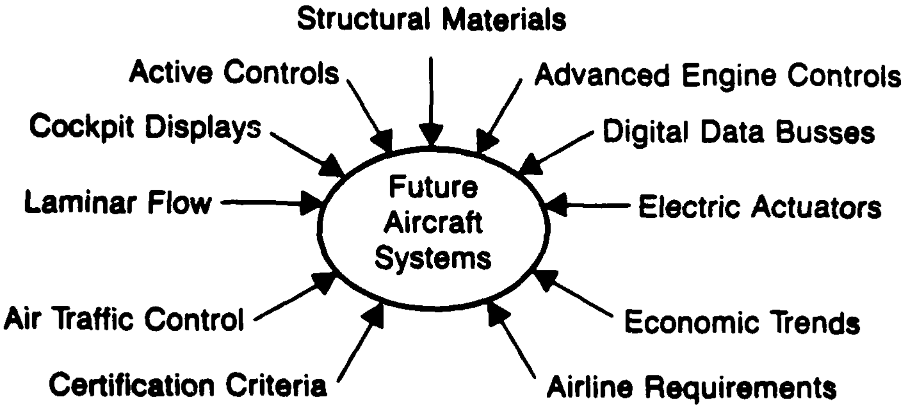


FIGURE 2.2-1. EMC AND AIRCRAFT SYSTEMS DEVELOPMENT

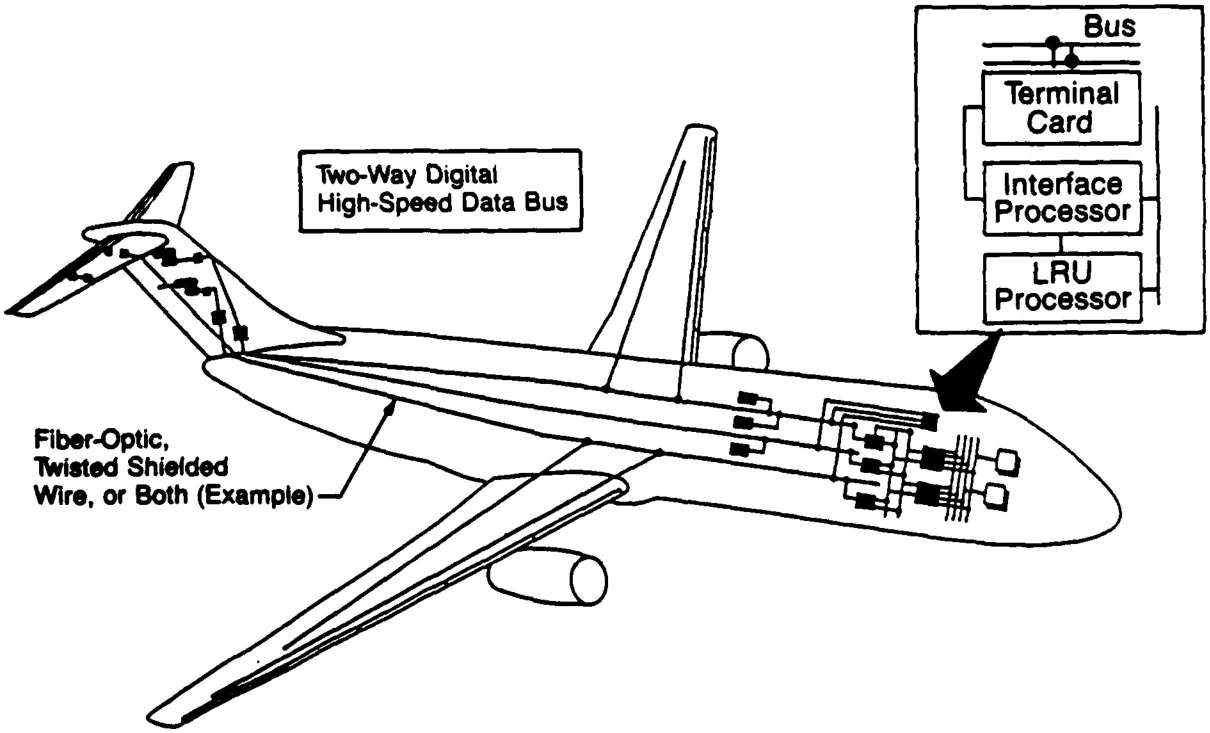

Bus
Terminal Card
Interface Processor
LRU Processor
Two-Way Digital High-Speed Data Bus
Fiber-Optic, Twisted Shielded Wire, or Both (Example)

FIGURE 2.2-2. DATA BUS ARCHITECTURE

There will be a number of new aircraft technologies that will moderate problems but will mean new areas of expertise and study:

- All-electric airplane (electric actuators), pulsed dc.
- Autonomous, multiple-access data bus with decentralized computers (dual redundant).
- Self-diagnostics, self-test, error control, and record keeping.
- Electronic keyboard actuation of power and avionics.
- Side-stick controllers.
- Single point-of-entry program loading.
- Flat-panel and head-up displays.
- Voice control.

What will be the impact of these systems on electromagnetic compatibility? More inductive switching transient control? Electrostatic transient control? Better high-energy radio frequency fields rejection and control?

Flat panel displays collocated with their own microprocessor avionics on the flight deck, depending on design, will mean less wiring and fewer coupling paths, less susceptibility, less electromagnetic radiation and electromagnetic interference. An improved flight management system will integrate navigation, communication, guidance, and energy management. Moreover, there will be expanded management capability of all of the systems (figure 2.2-3).

Multi-function keyboards will permit speed, flexibility, and maximum accessibility of options and data selection initiated by voice (figure 2.2-4). Side-stick controllers, electronic throttle, and flap control will not only facilitate operation and open up the instrument panel viewing area, but will also demand guarantees of safe operation and freedom from noise. Head-up displays and electronically-controlled relays and actuators will help clear and simplify instrumentation and add more power and versatility to aircraft control on the flight deck.

One of the key elements in a future aircraft is the data bus, where wire and weight savings will be dramatic. The number of interface circuits will decrease (figure 2.2-5). Research on digital buses will be required to better define susceptibilities to high-energy radio frequencies and transients. It is expected that some form of multiple access bus will be available for future aircraft (figure 2.2-6). Commercial transport planes are now using the ARINC 429 bus, a 12-kHz or 100-kHz, unidirectional, twisted pair, shielded bus that operates from each transmitter to multiple receivers with a binary-coded decimal format. The military bus is MIL-STD-1553: a 1-MHz, bidirectional, twisted pair, shielded, transformer-isolated bus totally run from a centralized 1553 bus controller with a serial, Manchester II, bi-phase format. (See section 10, Bibliography, ARINC 429 and MIL-STD-1553 bus system.) New systems are being developed to provide multiple access and decentralized processing. One such is called DATAC, a 1-MHz, bidirectional, twisted pair or fiber-optic bus with controlled specifications of protocol to facilitate transmission and reception.

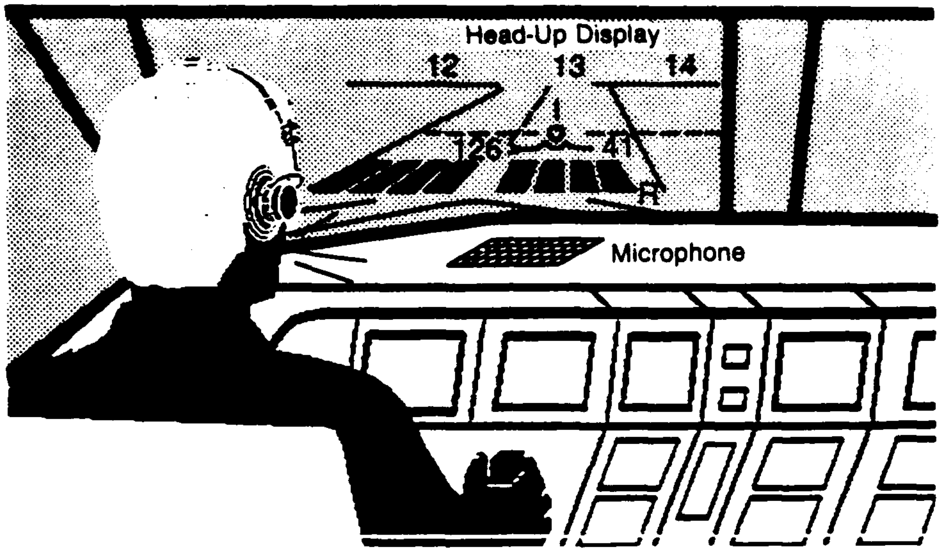


FIGURE 2.2-3. LINE-OF-SIGHT DISPLAY AND VOICE CONTROL

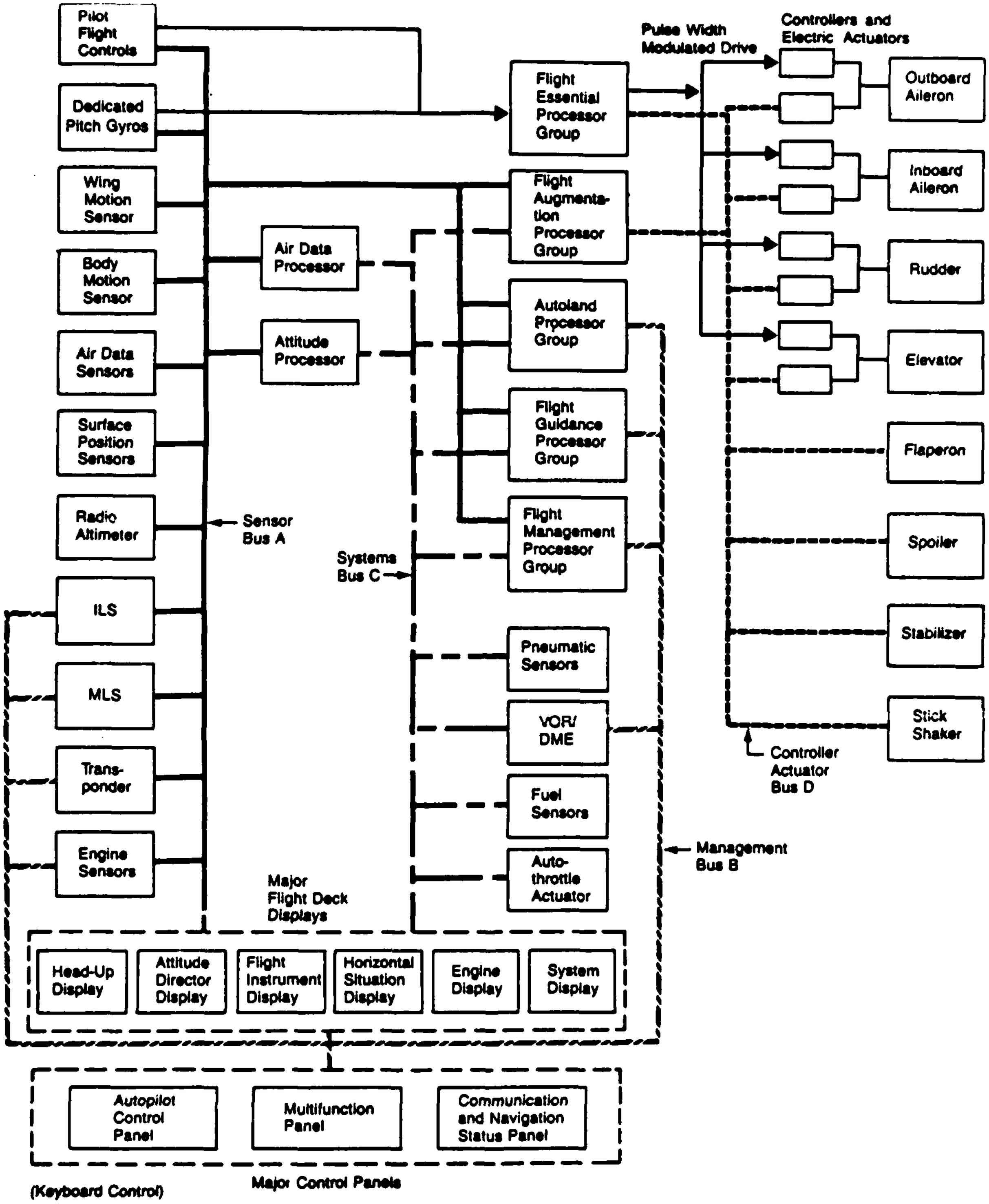


FIGURE 2.2-4. HYPOTHETICAL ARCHITECTURE

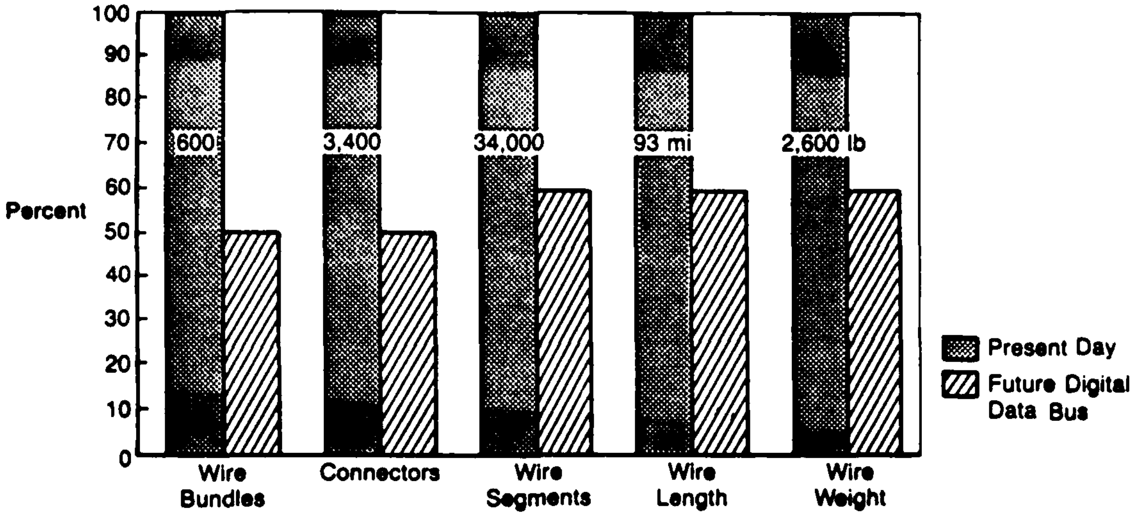


FIGURE 2.2-5. DATA BUS COMPARISON

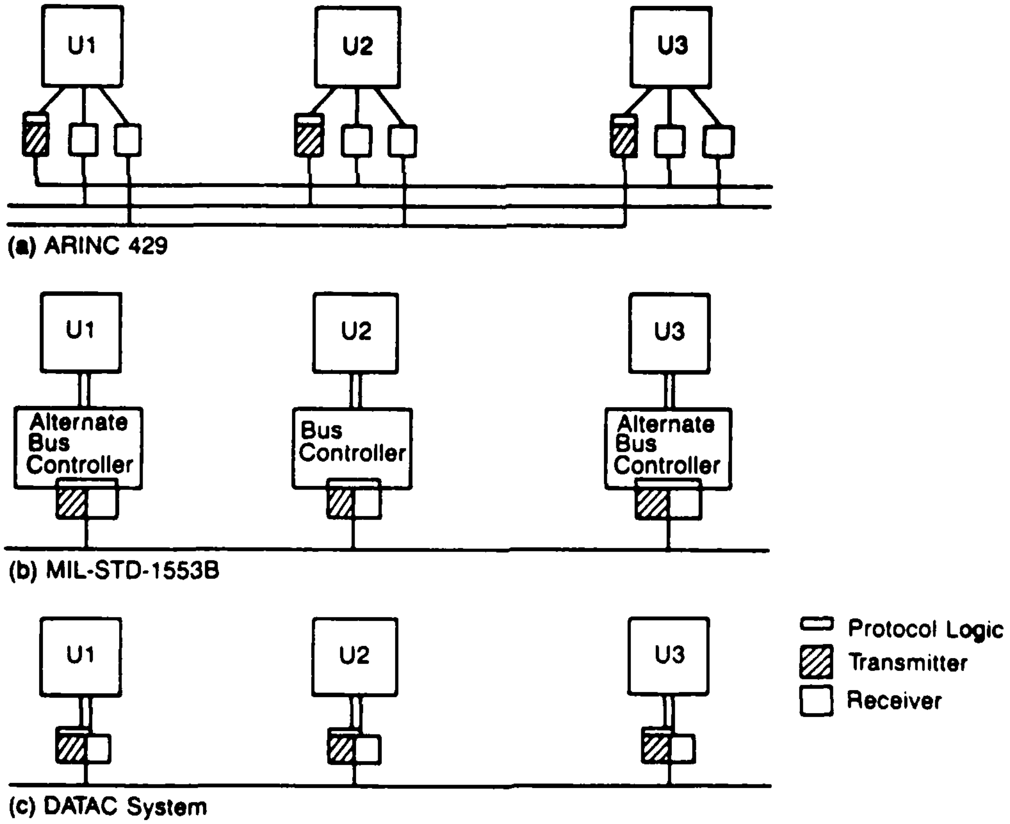


FIGURE 2.2-6. DIGITAL DATA BUSES

Possibly one of the most revolutionary changes to come about for electromagnetic compatibility will be the increased introduction of self-test and self-diagnostic capabilities in avionics allowing real-time readout or a history of equipment susceptibilities to noise (figure 2.2-7). Microprocessor evolution is speeding the development of these systems, and dramatic changes will occur in the immediate future (figure 2.2-8 and figure 2.2-9).

Hydraulic actuators powering control surfaces and other aircraft items such as landing gears and doors may be replaced by all-electric actuators now being developed. The actuator controllers contain "pulse width modulated" signals driving stepper motors. They are relatively high-voltage devices, are noisy, and the pulses need to be contained.

New composite and metallic alloy structural materials will mean greater efforts in the evaluation of the cornerstones of electromagnetic compatibility - the grounding and bonding designs that maintain current paths and stable electrical references (figure 2.2-10).

Many existing systems are being advanced and iaproved (table 2.2-1 and figure 2.2-11).

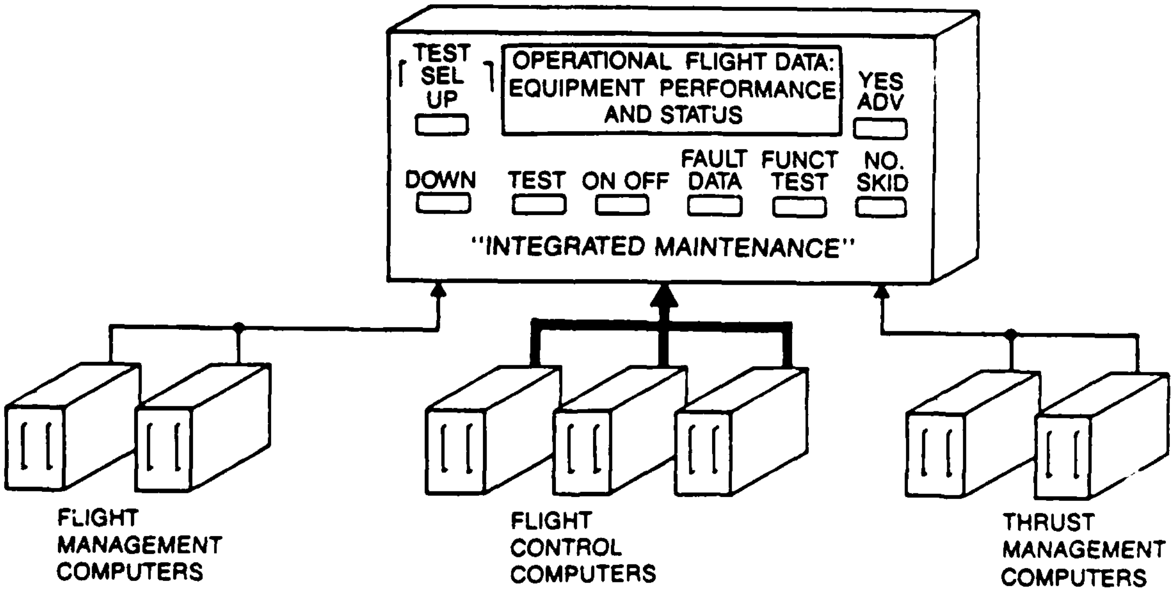


FIGURE 2.2-7 PERFORMANCE AND STATUS MONITORS

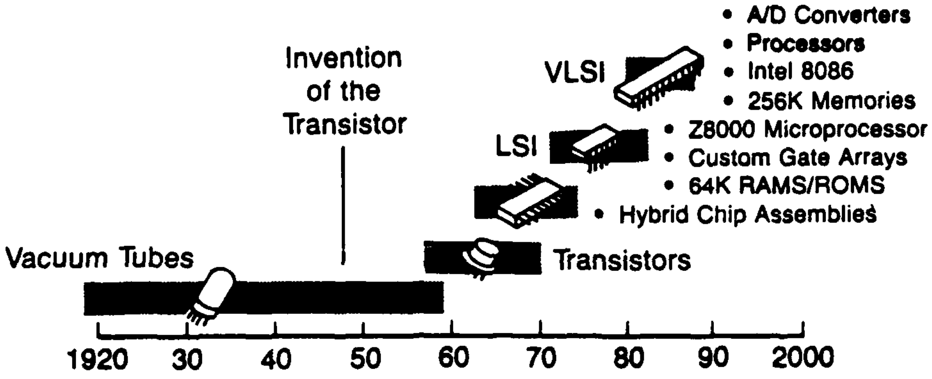


FIGURE 2.2-8. MICROPROCESSOR EVOLUTION

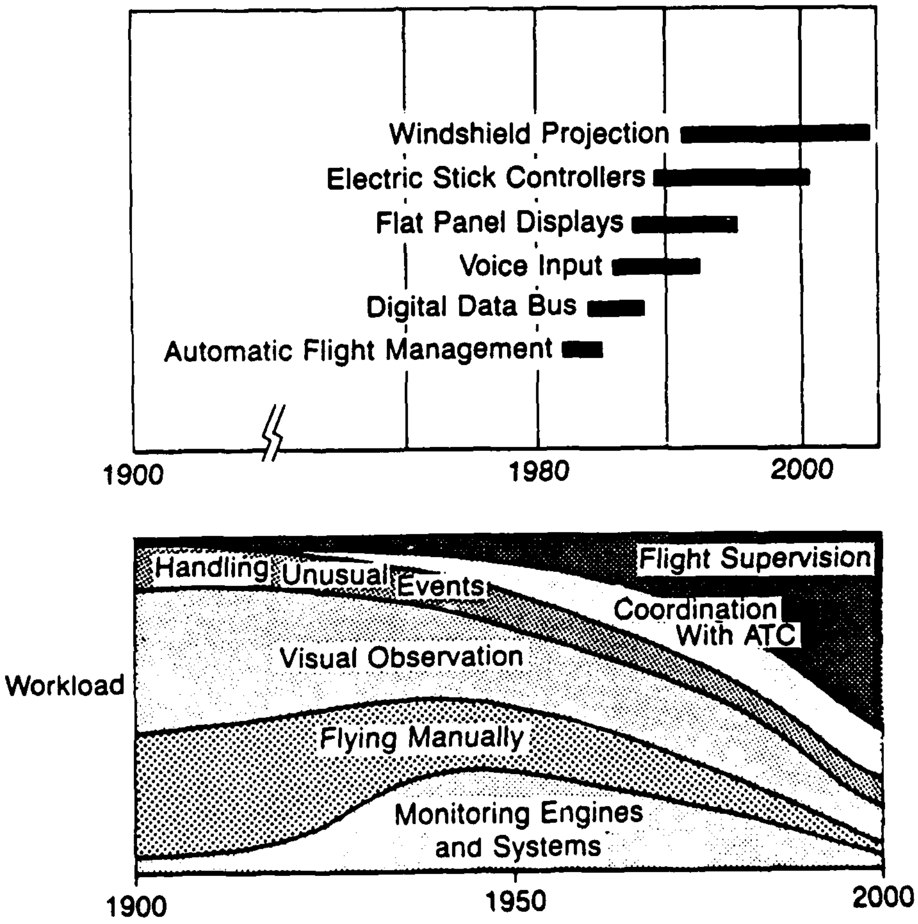


FIGURE 2.2-9. AVIONICS TECHNOLOGY PROGRESS

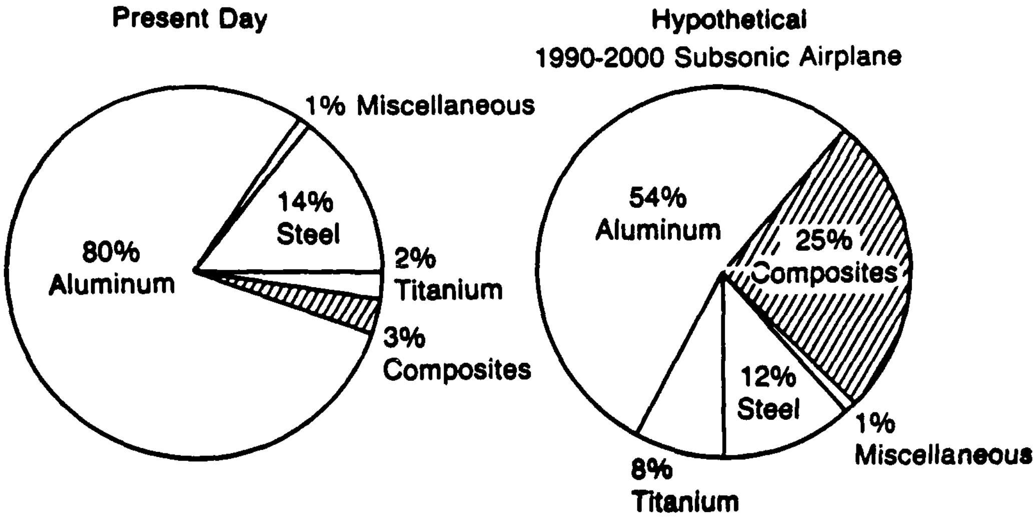


FIGURE 2.2-10. MATERIALS DISTRIBUTION

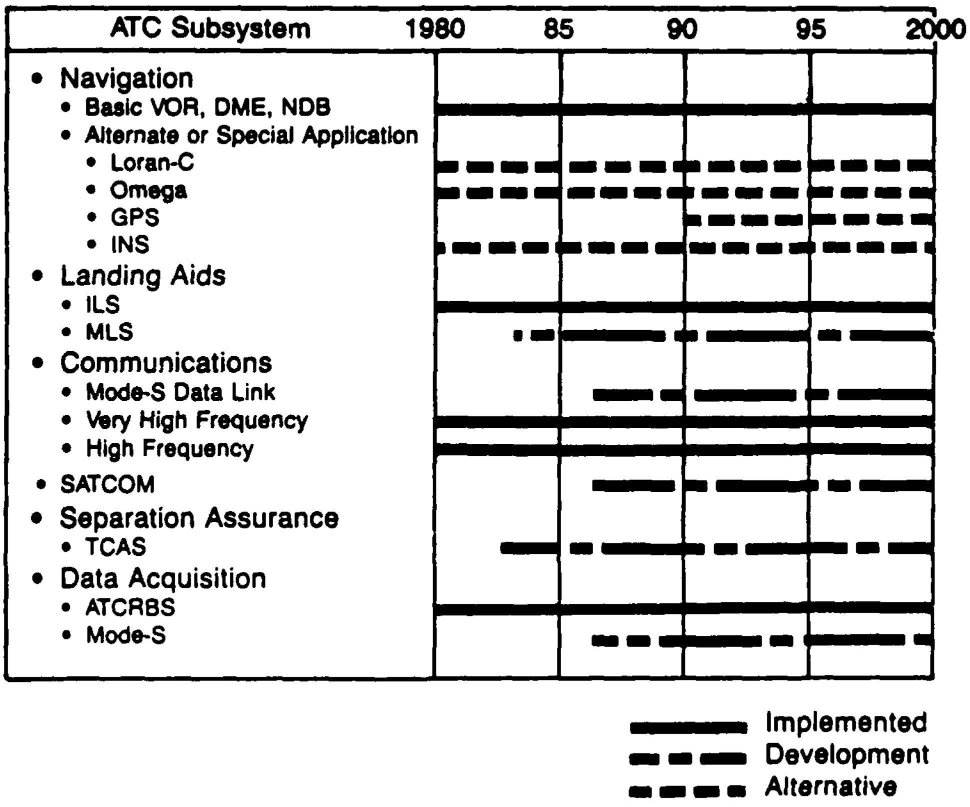


FIGURE 2.2-11. 1990'S ATC IMPLEMENTATION

TABLE 2.2-1. 1990's ATC IMPLEMENTATION

| SYSTEM | APPLICATION | AVIONICS |
|---|---|---|
| • DATA ACQUISITION | | |
| • ATCRBS WITH MODE-S | • Mode-S-Equipped Transponder Required on Air Carrier Aircraft | • Mode-S Transponder |
| • SEPARATION ASSURANCE | | |
| • TCAS | • Required for All Air Carriers | • Interrogator, Controls, and Displays |
| • COMMUNICATIONS | | |
| • VHF VOICE | • Most U.S. Domestic and Foreign ATC Operations | • VHF Transceiver |
| • MODE-S D/L | • High-Density U.S. Airspace | • Mode-S Data Link Modem and I/O Devices |
| • HF SSB | • Overocean and Lesser Developed Overland Air Routes | • HF SSB Transceiver |
| • SATCOM | • Overocean Voice and Data | • Data Unit and RF Unit |
| • NAVIGATION AIDS | | |
| • VOR | • Required for Short-Range Navigation | • Receiver |
| • DME | • Required for Short-Range Navigation | • Interrogator |
| • NDB | • Needed for Navigation and Approach Guidance in Some Areas | • Automatic Direction Finder |
| • INS | • Used for Long-Range Navigation Independently or With Other Systems (e.g., for Position Fixing) | |
| • OMEGA | • Used for Long-Range Navigation Independently or To Position-Fix INS in Either VLF or Omega Modes | One or More Types Needed for Long-Range Navigation; INS Installation Must Be at Least a Dual System |
| • GPS | • May Find use for Either Short- or Long-Range Navigation or To Position-Fix INS | |
| • LANDING AIDS | | |
| • ILS | • Required Until 1995 or Until All Destination Runways Have MLS | • ILS Localizer, Glideslope, and Marker Beacon Receivers |
| • MLS | • Required After 1995 but Needed Before To Obtain Improved Landing Guidance Available at Runways Where Implemented | • MLS Receiver |

The air traffic control radar beacon system (ATCRBS) operation (based on a ground interrogation of an airplane transponder to assess flight identity, altitude, range, and azimuth) is being upgraded with a new beacon mode, called Mode-S, which is a two-way digital link, to selectively address each aircraft. Surveillance en route and at terminals during approach starts at about 6000 ft (1830m) above ground level.

The airport surface detection system (ASDS), a primary radar system, is being implemented to transmit a pictorial presentation of the terminal surface area in order to expedite traffic.

The Instrument Landing System (ILS) consists of a 108- to 112-MHz localizer for horizontal, a 328- to 335-MHz glide slope for vertical, and two 75-MHz marker beacons for distance to provide position starting at 33 km from the runway (18 nmi). The system is used extensively and will be augmented with a new Microwave Landing System (MLS) to provide landing in zero visibility utilizing a ground-transmitted signal to the aircraft to establish elevation, azimuth, and distance and is now collocated with the MLS until replacing it.

Navigation systems will expand in extent and capability. The Traffic Alert and Collision Avoidance System (TCAS) requires a transponder trace, and interrogator to detect, track, and compute aircraft flight path projections and initiate selected levels of warning and avoidance maneuver advisories.

The Very High-Frequency Omnidirectional Range (VOR) establishes a magnetic bearing, is a short-range aid, and is generally collocated with a Distance Measuring Equipment (DME) station, which provides for more precise distance measurement from the VOR.

The Automatic Direction Finder (ADF) uses nondirectional beacons (200 to 415 kHz) to provide a bearing (± 3 deg) at a range of 18 to 650 km (10 to 350 nmi).

Loran-C covers about 1850 km (1000 nmi) with pulses at 100 Hz with a positioning accuracy of 0.46 km (0.25 nmi), repeatable to 18m to 90m (60 to 300 ft) and is operated by the Coast Guard along the contiguous U.S. and Alaska, but is presently not being installed by scheduled air carriers.

Many of these systems will be supported or replaced by the Global Positioning System (GPS) which in future years will provide worldwide, accurate, all-weather positioning.

Communication systems will see unparalleled improvement in reliability and flexibility.

Very High-Frequency (VHF) voice communication, the continental U.S. air traffic control system to airport towers and control centers, operates between 116 and 136 MHz with projected bandwidth spacing of 25 kHz at a receiver sensitivity of around a microvolt.

High-frequency (HF) voice communication, for use over water, operates at 2 to 30 MHz with a receiver threshold of about 2$\mu$V and transmitter output of possibly 400W peak effective power.

## 2.3. Criticalities

### 2.3.1. Measures and Definitions

By any measure, airplanes are safe. Airplane avionics are a part of that safety picture. And electromagnetic compatibility is a part of the proper operation of avionics.

Although safety records have been built and established over the years, the criticality of avionics and their interconnecting wiring is not an unchanging situation. Of course, mathematically finite possibilities of avionics performance errors or malfunctions always exist, and it almost goes without saying that absolute, definitive resolution of the exact probabilities and reliability of critical circuits is elusive.

"The simultaneous failure of two reliable independent systems, each of which has dual redundancy," states FAA Advisory Circular AC No: 25.1309-1, "is expected to be extremely improbable." But still, the performance of critical avionics equipment cannot be allowed to be affected by the noise in the airplane.

Critical circuits need evaluation. Evaluation is needed on non-essential systems for their effect on critical circuits. Flight crews must not be given misleading information. Noise effects can be barred with shielding, rejected by balanced circuits, diverted and contained with filtering, or neutralized by software.

Table 2.3-1 itemizes some equipment criticality categories and definitions, and figure 2.3-1 charts a general relationship of probability and consequence.

TABLE 2.3-1. CATEGORIES OF CRITICALITY

| Category | Function | Impact | Probability of Occurrence | |
|---|---|---|---|---|
| A | Critical | Prevent safe flight | Extremely improbable | $\leq 10^{-9}$ (per 1 hr.) |
| B | Essential | Impaired ability to cope | Improbable | $\leq 10^{-5}$ to $> 10^{-9}$ |
| C | Nonessential | No significant degradation | May be probable | $> 10^{-5}$ |

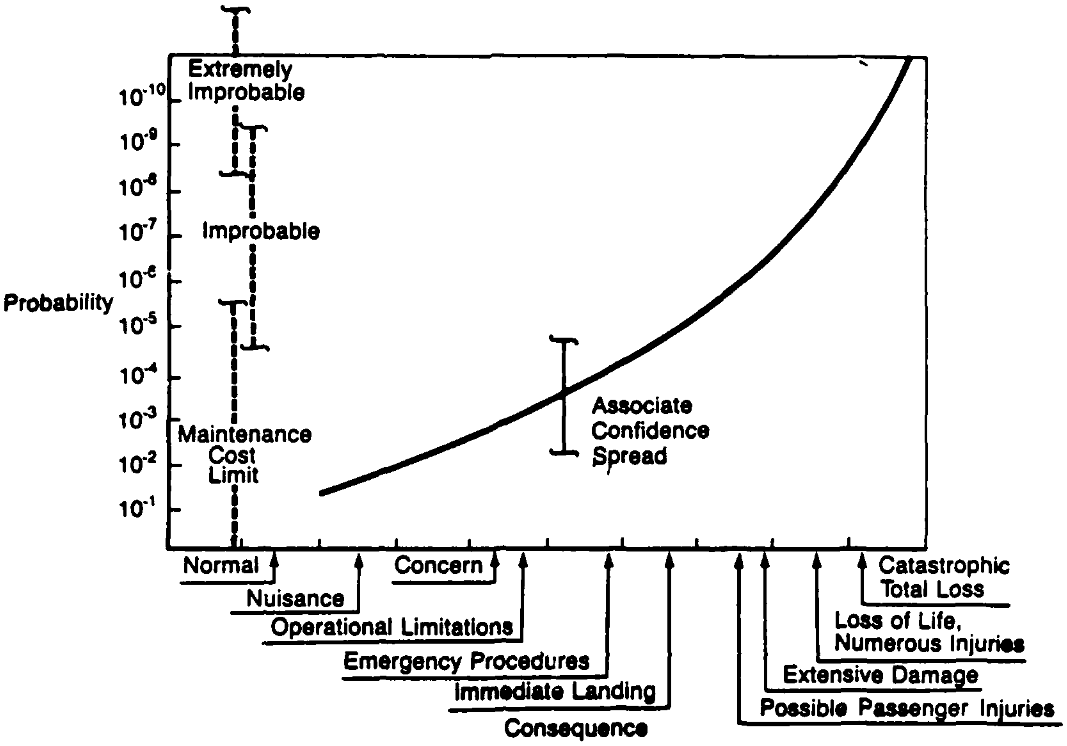


FIGURE 2.3-1. PROBABILITY VERSUS CONSEQUENCE

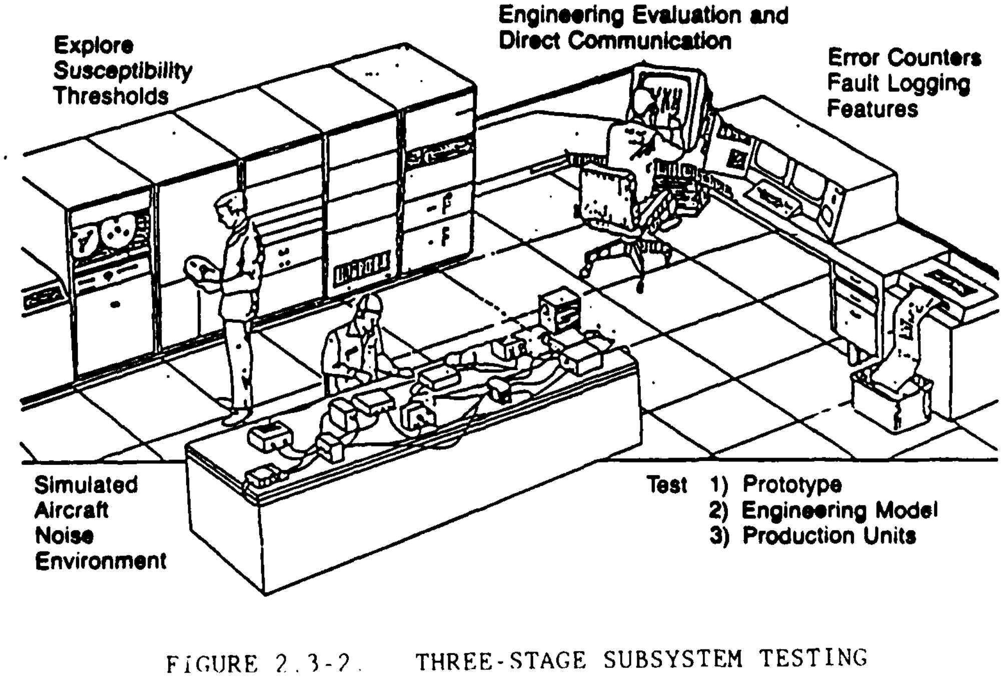

Explore Susceptibility Thresholds
Engineering Evaluation and Direct Communication
Error Counters Fault Logging Features
Simulated Aircraft Noise Environment
Test 1) Prototype
2) Engineering Model
3) Production Units

FiGURE 2.3-2. THREE-STAGE SUBSYSTEM TESTING

Toward the end of an airplane program, malfunctions or upsets can practically be brought to zero by repeated subsystem testing by the airframe manufacturer in conjunction with the avionics manufacturer of, first, prototypes, then engineering models, and finally production units. The avionics operation in a simulated noisy environment will be understood, and verified, and the data and experience will help contribute to aircraft validation (figure 2.3-2).

## 2.3.2. Critical Equipment

What makes equipment critical? What conditions influence criticalities? Here are some defining generalities:

Function:

- Does the unit support safety of flight or is it for convenience, comfort, work relief, or economy?

- Is the unit employed to maintain flight, or is it needed to proceed to the nearest airport, or to continue to destination?

Redundancy:

- Is the unit triple or quadruple redundant?

- If the first unit fails and the second unit fails, can loss of aircraft be averted?

*History:*

- What is the history, condition, and age of the unit or the aircraft?

- Are all units operating at flight dispatch?

Flight conditions:

- Is criticality based on phase of flight: takeoff, climb-out, cruise, landing?

- Is criticality based on type of flight: deficient or lack of navigation facilities, instrument flight, heavy weather, long flight, over water, nighttime operation?

- Is flight safety dependent on automated electronic controls, instruments and sensors?

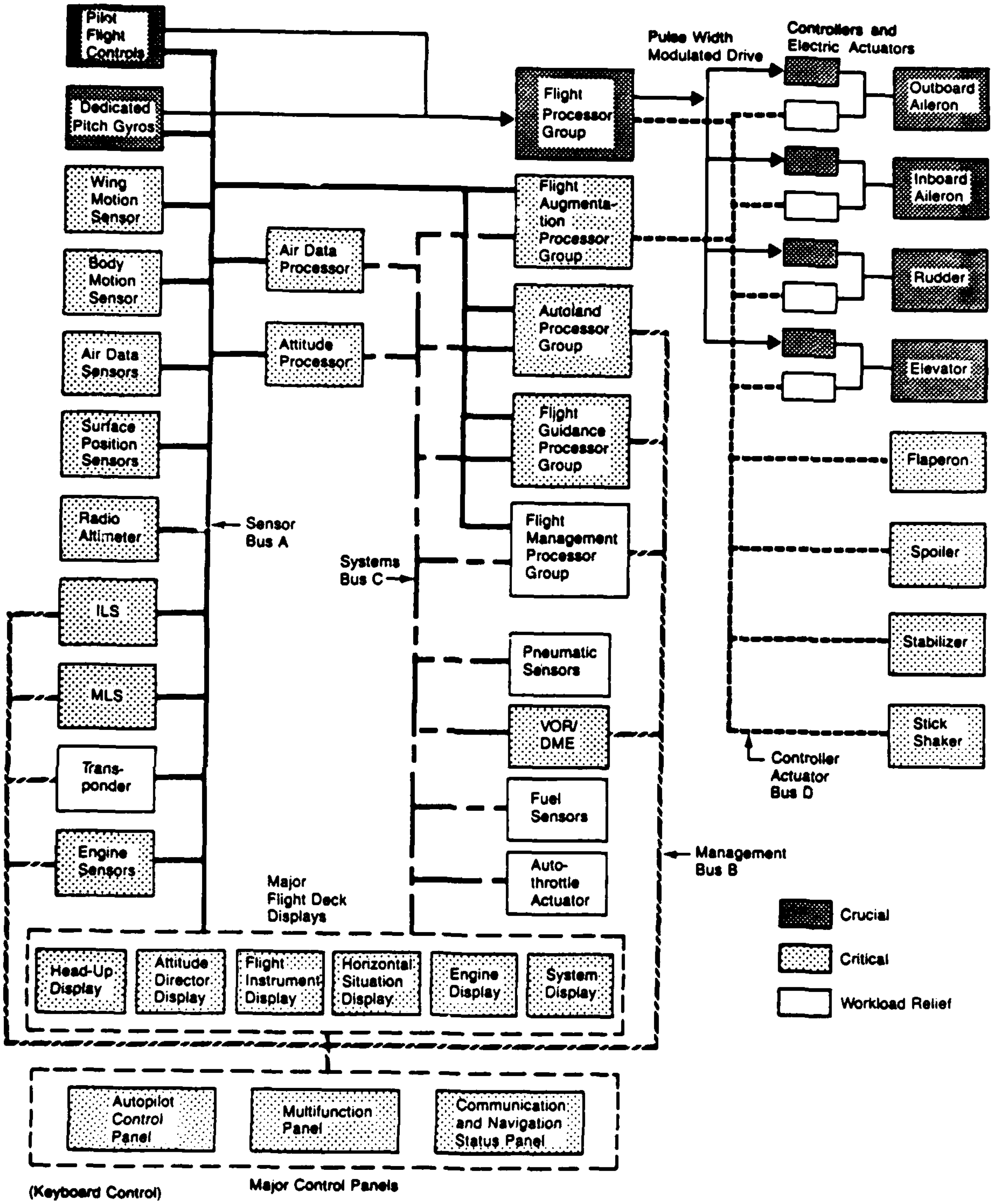


FIGURE 2.3-3. PROJECTED CRITICALITIES

What circuits are classified as critical? Certain circuits or functions must be extracted and given special attention for electromagnetic compatibility. Circuits that might be considered include these illustrative examples:

- Flight control/flight management: control surface actuators, displacement transducers, servo valves, position indicators, switches/valves; electric controllers/actuators; negative stability controllers; augmentation controllers; air data, attitude, altitude, airspeed, and situation indicators, displays, control panels and their backups; automated landing system.
- Navigation/communication: VHF transceivers, voice recorder, tape recorder, ADF, radio altimeter, instrument landing system, marker beacon.
- Power: standby power, instrument lights, standby instruments.
- Advisory flight instrumentation: actuators, position indicators, displays, test circuits, pressure, temperature, quantities.
- Fire detection systems.
- Landing gear: antiskid control.
- Engine: controller actuators, computers, displays, temperatures, speeds, pressures, quantities, restart/shutdown, thrust reversers.

Figure 2.3-3 delineates a block diagram of some hypothetical categories of future aircraft systems.

## 2.4. Packaging and Architecture

The aircraft is an electrical/electronic package. Right from the start, the aircraft packaging design must include a layout and topology that optimizes electromagnetic compatibility. Here are the dominant EMC desired designs:

- Major subsystems are grouped together for an in-line equipment design, input to output, to draw out the shortest possible wire bundle routing.
- Major incompatible wiring groups are separated: power feeders from electronics; analog (with single point ground) from digital; high voltage/high frequency from digital; low-level sensitive from power.
- The aircraft has a designed system-level shielding barrier combined with a designed, controlled, equipotential ground plane system.
- Every interface circuit, electronics and power, is filtered and prote^cted. Controlled transmission line design techniques are employed for susceptible and digital interface circuits.
- Every installed unit of equipment meets the EMC qualification test requirements.

All of these designs and technologies need early conceptual consideration, planning, and lay-out. A mockup is invaluable. In-line design is the best. Locate equipment to minimize wiring lengths. Electromagnetic coupling increases with length. Make wire connections short. It's good for weight. It's excellent for electromagnetic compatibility.

Here is a more detailed checklist.

Grounding:

- Ground connections cleaned and burnished, no paint, must verify.
- Ground wires evaluated for resonance, capacity, and continuity.
- Avionics case grounded with a low resistance (and verified).
- Grounding paths and references designated on drawing.
- Trays, conduits, metal liners, foils designed for return currents.
- Graphite-epoxy not used as structure return.
- Analog circuits are single point grounded or isolation provided.
- Each avionic unit return/ground identified.
- Engine circuit return/ground analyzed for wire length and impedance.

Bonding:

- Structure electrically bonded and aperture bonds confirmed.
- Electrostatic conductive paints applied to external dielectric or nonconductive surfaces.
- Equipment bonding to structure verified.
- All isolated metal objects bonded.

Shielding:

- 360 degree, peripheral shield connections used.
- Backshell continuity defined and checked.
- All circuits evaluated for shielding.
- All low-level, sensitive circuits shielded.
- Shield noise not carried inside case confirmed.

Wiring:

- Landing gear wiring installed in conduit and flexible overbraid.
- No wiring routed under unshielded fairings.
- Wiring installed close to structure.
- Shielded, balanced, isolated interface circuits employed.
- Power feeders given a power line and a wire return.
- Signal lines given a signal line and a wire return.
- Twisted pair used for audio circuits.
- Oscillator harmonic frequencies emanating from clocks, switching regulators, pulse width modulators, and digital data lines shielded. Conducted and radiated emissions, close to receivers, may need to be controlled below DO-160 limits.

Packaging/installation:

- Test data dug out to verify equipment complies with specification.
- Equipment tested to up-to-date requirements.
- Transformers separated from CRTs and audio circuits.
- Environmental control, flight control/electric actuators, flight management, radio transmitters and receivers, power, and engine control systems unearthed, defined, grouped, and aligned.
- Mockup constructed to settle on equipment topology.
- Functional or subsystem grouping provided for environmental control electronics, switching units, valves, fans; flight control, electric controllers located next to stepper motors; air data, caution advisorv computers next to their transducers; radio frequency units, power supply, electronics, amplifier, antennas; heavy power generators, converter regulators, transformer rectifiers, switching contactors, power switching unit installed together, and separated from avionics; power "single point grounds" positioned next to power regulator or distribution unit; power switching unit centrally located; dedicated avionic power supplies installed next to the unit they supply; electronic engine controllers positioned to shorten and minimize wiring to engine sensors and controls.
- All circuits evaluated for filtering.
- Equipment input and output wiring not doubled back upon itself.
- All circuits evaluated for categories and separation.

These are not all the answers but they will help.

## 2.5. Issues

### 2.5.1. An Early Start

The whole EMC scenario rises up and needs resolution at the concept of the program. This is an issue. The scope and depth are resolved first - is it a proposal? - proof of concept? - or full production program? What are the funding boundaries?

Environmental assessment quickly follows, all of the environment inside and outside of the airplane. This is an issue.

Early in the program, light must be shed on the "tailored" design requirements or waivers for subcontractors. New systems demand definition. Policy and schedule come into focus in a brief EMC plan. These are large tasks and they are all at issue. Bringing two or three people on board early is an added expense. It seems unnecessary. Electromagnetic compatibility design does not start at the design stage, it starts at the concept stage.

### 2.5.2. Design

#### 2.5.2.1. Shielding

Shielding is one of the best ways, the most all-around effective ways, to protect a circuit. Shielding diverts almost all of the energies of noise. Shielding stops transients as well as radio frequencies. It protects against electric fields. It helps to maintain controlled stripline impedance. It guards against arcing and sparking. But, it adds weight to the aircraft, requires maintenance, and costs more. Shields require shield ties - difficult to install, particularly for panel-mounted equipment. With adequate modeling and design effort, shielding can be judiciously applied.

#### 2.5.2.2. Power and Signal Returns and Wire Grounds

Sometimes a wire is good, sometimes bad. Many of today's circuits or case housings are referenced to structure ground with a wire, which may resonate. Many of the interface circuits between pieces of equipment do not have a wire return, which will open the circuit up to noise. Both of these practices are detrimental to EMC, but they save on weight. Wiring is good as a signal return and bad as a circuit reference.

#### 2.5.2.3. Dielectrics

By specification, wiring and connector insulations have dielectric withstand strengths at sea level ot 1500V 400-Hz steady state. That 1500V weakens as one goes up in altitude. It can be down around 300V its lowest point, at an altitude of 250,000 ft. In the future, as power line voltages rise and aircraft altitudes increase, dielectric strengths and corona will become more of a concern.

### 2.5.3. Environment and Test

#### 2.5.3.1. High-Energy Radio Frequency Fields

Magnitude, pattern, frequency, polarization, modulation, and geographical location of high-energy radio frequency and radar transmitters are needed. To evaluate aircraft circuit immunity, a systems approach must be implemented to study shielding, induced voltages, circuit protection, and software correction techniques. An industry susceptibility test specification is needed. In areas such as this, compliance to DO-160 may not guarantee system-level compatibility. Efforts are underway to provide an update of high-energy radio frequency field environments and protection techniques. (See section 10, Bibliography, ECAC study on Electromagnetic Environment.)

#### 2.5.3.2. Fields From 400 Hz and Transients

Some say that the power system 400-Hz is the most troublesome electromagnetic environment on the aircraft causing 50% or more of the shortcomings in EMC quality. Audio 400-Hz "hum" derives from magnetic ("H") field. Electric ("E") fields can trigger a comparator circuit that has high-input impedance, and it is well known that powerline transients cause logic upset resulting in lockup or even equipment shutdown until the flaws are found and rooted out. Through better definition, analysis, and modeling techniques, avionics designers must be made aware that their equipment is operating in this environment. Higher design and test levels are appropriate in some instances, coupled with more attention to finding interface circuit thresholds during test. It is controversial.

#### 2.5.3.3. Test Conditions

In the laboratory during development or qualification testing, it is expensive, difficult, and meaningless to strive to recreate actual aircraft installation or production configurations. There are wire lengths, resonant conditions, and test coupling conditions that may not adequately simulate the aircraft and, because of this test deficiency, may ultimately lead to an upset occurring on the aircraft. Possibly one answer is to verify that test levels are high enough with an adequate safety margin. Subsystem tests offer information on EMI characteristics to help moderate this dilemma. Aircraft tests authenticate the final EMC design.

#### 2.5.3.4. Emission Variances

Today's conducted and radiated emission limits are restrictive under some conditions (see section 9). Computers, with digital clocks and switching regulators, sometimes emit harmonics in the HF megahertz region that defy total containment and consequently emissions may be a few dB above limits. Cases exist where it is uneconomical and unnecessary to go to extraordinary efforts to filter those emissions if it can be shown that they will not in any way radiate to local receiving antennas. Infringements may be approved and deviations granted without adverse effects on neighboring circuits. The present radiated emission limit in the VHF range is not too restrictive and, in fact,

#### 2.5.3.5. Subsystem Testing

Subsystem testing is different in intent from equipment qualification testing. Subsystem testing, usually held at the airframe manufacturer's facility with support from the avionics supplier, provides insight into the susceptibility thresholds and emission levels while simulating noise environments of the airplane.

The tests are for engineering evaluation and they provide significant information on computer processing performance and interface data quality. Test software exercises the processing functions and the interfaces between avionics units, and further, it monitors processing, memory, and transmissions of data for any abnormal conditions. Error counters or fault logging features examine operation in real-time and provide capability for hard copy printout. Formal pass or fail standards for susceptibility and emission do not apply. Completion of the specific test procedures and the investigation is the gauge for determining success.

The features are that many interface circuits are per manufacturer's configuration, software is up-to-date, and observation is real-time. At this stage of the program, the equipment avionics engineer is available to provide rapid evaluations and judgments. Re-evaluation and decisions on rework or test changes are easy and flexible. Often these tests can be performed on a "non-interference" basis using informal procedures. They establish standards for the airplane test. Costs are low.

#### 2.5.3.6. Aircraft Testing

Aircraft testing is the final authentic proof. It offers first hand "real-world" validation. Wiring, equipment, and installations are the final design. It is expensive, however. It is expensive beginning with the test procedure (step-by-step development and approvals), then the aircraft test itself (a labor intensive operation compounded on top of a costly unit of equipment), then continuing with the formal documentation of unplanned events during the test, and ultimately ending with an elaborate final report.

### 2.6. Variances in Electromagnetic Compatibility

#### 2.6.1. Diagnostics and Troubleshooting

Flight test phoned project. Project called flight deck instrumentation staff. Then staff contacted the electromagnetic compatibility engineers.

A new aircraft on the flight line had a discrepancy in the left engine fuel flow reading. The fuel flow digital readout on the display screen of the criticality advisory system (CAS) was variable and erratic whenever the 400-Hz power to the enginc Mach probe heater was energized. What was happening and what was the cause? A work authorization was quickly approved; time on the airplane scheduled; and laboratory test support called in.

On the airplane, in cramped quarters next to the electronics bay, investigators used an oscilloscope to troubleshoot the problem on the circuits running from the fuel flow meter on the left wing engine to the CAS computer located in the electronics bay. Connectors were hard to reach and remove with care. Knuckles got scraped. Equipment was difficult to move. Engine run time was expensive. As a part of the investigation, the left engine wire bundle was disconnected from the left CAS computer and reconnected to the right CAS computer to see if the problem would "follow" the bundle. It did, and that showed that the CAS computer itself was not totally at fault and that 400-Hz, 115V power in a wing wire bundle was being coupled to the fuel flow circuit.

The 400-Hz, 115V power wire to the mach probe heater, traced out on the wiring diagrams, starts in the electronics bay and runs out to the engine; but then the 115V heater return wire is taken from the engine back onto the engine strut; the wire is there connected to structure with structure being used as return back to the power source in the electronics bay. So the "high side" of the 115V power wire runs in the same bundle in the leading edge for 100 ft next to the unshielded, fuel flow circuit. There is 100 ft of "electric field" capacitive coupling.

On the other hand, the fuel flow circuit is three wire balanced, has the meter wires isolated on the engine, and has a high-resistance input to an operational amplifier in the CAS computer protected at the input by 5 kΩ resistors and diodes to ground. The two, 350-mV pulses generated by the fuel flow meter have a working period approximating the period of the 400 cycles per second. The 115V 400-Hz noise was induced right on the 350 mV.

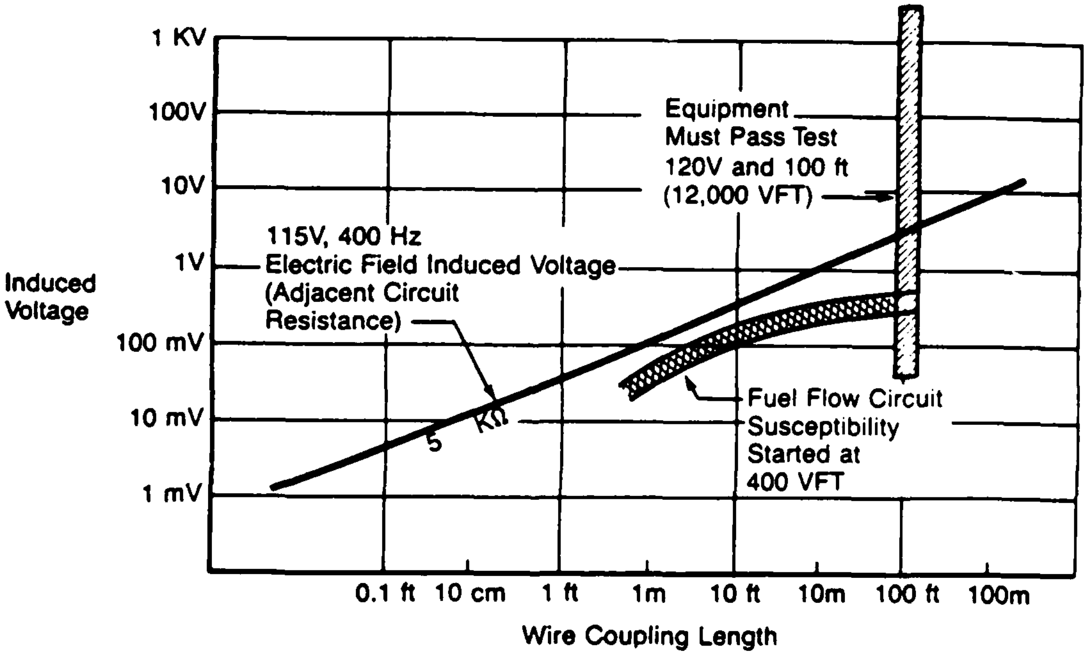


FIGURE 2.6-1. A DISCREPANCY

The fuel flow circuits were rapidly set up and simulated in the laboratory and they malfunctioned under the DO-160 power line "electric field" test just as had occurred on the aircraft. It took only 40V at 10 ft (400 Vft), equivalent to 4V at 100 ft, of coupling to cause upset (figure 2.6-1). The test requirement is 120V at 100 ft (12,000 Vft). Other DO-160 tests caused no upset. Once the simulated circuits with the proper pulses had been developed and the thresholds and boundary characteristics of the upset outlined, the test was scheduled, set up, and run in an avionics laboratory with a production configuration CAS system. With management approval, communication was established through Project with the subcontractor. He was able to duplicate the condition.

The long, 100-ft wiring run, all the way from the electronics bay through the wing pressure seal, then along the wing leading edge to the engine strut and down into the engine, had provided an extensive opportunity for electric field coupling into the operational amplifier wiring. What will correct electric field coupling? A low resistance or shield will.

Wire shielding, installed on the airplane fuel flow circuit, provided an excellent barrier against the electric field and was a quick solution.

The operational amplifier design in the CAS computer, although a balanced circuit, did not offer proper noise rejection to stop the upset. It turned out that that circuit design was inherently difficult to balance, partly because of resistor mismatch, partly because of capacitor imbalance, and possibly because of a phase shift occurring in the signal return.

This "variance" from electromagnetic compatibility on the aircraft took months to resolve. Flight test, project, manufacturing, management, and subcontractors: all were involved. Work authorizations, reviews, justifications, and documentation were invoked, processed, approved, and completed. A necessary, but costly, effort.

### 2.6.2. Table of Variances

#### 2.6.2.1. Commercial

Diagnostics and troubleshooting of electronics are continuously demanded because of avionic circuit susceptibility to transients, 400-Hz electric ("E") and magnetic ("H") fields, radio frequencies (HF-VHF) including clock and switching regulator harmonics, and power quality. Knowledge of past lessons may help save design and troubleshooting expense (table 2.6-1). The bottom line is adequacy of specifications. In table 2.6-1, under the DO-160 column, recommendations are made on possible increases in test levels to improve aircraft electromagnetic compatibility.

#### 2.6.2.2. Air Force

The Air Force has documented troubleshooting experience. "The coupling of fields through the unintentional antennas formed by aircraft wiring," Zenter, the author, says, "is the cause of many interference problems." (See table 2.6-2).

## TABLE 2.6-1. VARIANCES IN EMC

| EMI CLASSIFICATION | SOURCE | EQUIPMENT RECEPTOR | PATH | SYMPTOMS | REMEDY | DO-160 |
|---|---|---|---|---|---|---|
| Static: | 1 windshld | captr | dsch | dis captr | gnd wndshld | add test |
| | 2 covers/pan | VHF rcv | • | aud | bnd covers | |
| | 3 duct | ADF rcv | • | • | gnd duct | |
| | 4 ant cover | • | • | • | paint covr | |
| Sw.trnsnt: | 1 powerline | captr | wc | del rud/ dis captr | lgnd | inc trnsnt |
| | 2 | • | • | lock up | cap/softwr | |
| | 3 | • | • | false cmd | • | |
| 400Hz "E"field: | 1 powerline | captr | • | ind- FF | shld | inc "E" field level |
| | 2 | N2 ind | • | ind- N2 | • | |
| | 3 | captr | • | ind-F/qty | • | |
| | 4 | aud cir | • | aud | • | |
| 400Hz "H"field: | 1 powerline | intrphn | gl | • | lgnd | inc "H" field level |
| | 2 | headset<br>VHF rcv | • | • | • | |
| | 3 | videocoax | • | del CRT | Tfx iso,lgnd | |
| | 4 | CRT | wc | • | TP & sep | |
| | 5 | tape head | • | aud | • | |
| | 6 | aud cir | • | • | fil,sep | |
| | 7 | • | • | • | TP,sep,lgnd | |
| Clock hrmncs: | 1 wx rdr | ILS rcv | • | • | sep | inc RF level |
| | 2 portble rad/rcdrs | omega rcv | • | ind del: spd,course | shld | |
| Sw.reg.hrmncs: | 1 captr | VHF rcv | • | aud | sep, shld | inc RF level |
| HF-VHF freq: | 1 VHF tx | handset | RE | • | fil micrphn | inc RF level |
| | 2 VHF tx | headset | • | • | tfx iso | |
| | 3 HF tx | captr | wc | cab press | fil, cap | |
| | 4 • | aud cir | • | aud | dublshld | |
| | 5 • | • | • | ind | • | |
| | 6 HF eq | VHF eq | • | aud | • | |
| "Crosstalk": | 1 VHF, DME | aud cir | • | • | sep,lgnd | |
| Radar: | 1 airport rdr | prx sw | RE | ind lts | shld | |
| Power qualty: | 1 powerline | captr | 28vac | ind | fil | |
| | 2 | • | 115v | no-land | • | |
| | 3 | • | • | pwr intrpt | cap, softwr | |
| | 4 | • | • | del CRT | softwr | |

ant-antenna
aud-audio hum or tones
cab-cabin
cap-capacitor
captr-computer
CRT-cathode ray tube
del-change or movement
dis-disengage
dsch-discharge
"E"-electric field
eq-equipment
FF-fuel flow
fil-filter
gl-ground loop
lgnd-single point ground
"H"-magnetic field
HUD-head up display
inc-increase
ind-indicator change
intrphn-interphone
intrpt-interrupt
iso-isolate
lt-light
N2-engine speed
prx-proximity switch
rad-transceivers
rcdrs-recorders
rcv-receiver
rdr-radar
RE-radiated emission
sep-separation
shld-shield
sup-suppression
tfx-transformer
TP-twisted pair
trnsnt-transient
tx-transmitter
wc-wire coupling
wx-weather

TABLE 2.6-2. AIR FORCE VARIANCES

| EMI CLASSIFICATION | SOURCE | EQUIPMENT RECEPTOR | PATH | SYMPTOMS | REMEDY | MS461 |
|---|---|---|---|---|---|---|
| Static: | 1 canopy | UHF rcv | dsch | aud | sep | add test |
|  | 2 " | " | " | " | bnd,gnd |  |
|  | 3 ant | " | " | " | " |  |
|  | 4 " | " | " | " | " |  |
| Sw.trnsnt: | 1 powerline | cmptr | wc | ind-rdr warn | shld,fil | add test |
|  | 2 |  |  | IFF code tx | diode sup, |  |
|  | 3 |  |  | ind-HUD cam op | softwr |  |
|  | 4 |  |  | bomb disarm |  |  |
|  | 5 |  |  | ind-flare |  |  |
|  | 6 |  |  | del-cmptr memry |  |  |
|  | 7 |  |  | ind-teran fol rdr |  |  |
|  | 8 | intphn |  | aud |  |  |
| 400Hz"E"field: | 1 powerline | omega rcv | RE | ind-del | sep | add test |
|  | 2 | VLF rcv |  | aud | fil |  |
| 400Hz"H"field: | 1 powerline | intrphn | wc | aud | lgpd | inc "H" |
|  | 2 | cmptr |  | del CRT | sep | field |
|  | 3 | " |  | ind oxy | " | level |
| Clock hrmncs: | 1 cmptr | ant | RE | aud | fil,shld |  |
| Sw.reg.hrmncs: |  | --none |  |  |  |  |
| HF-VHF-UHF: | 1 tx | cmptr | RE | del-cntrl surfce | fil,bnd,shld | inc RF |
|  | 2 | wiring |  | del-steer gear |  | level |
|  | 3 | " |  | del-rdr ant |  |  |
|  | 4 | " |  | del-winch |  |  |
|  | 5 | " |  | del-eng speed |  |  |
|  | 6 | " |  | ind-altimeter |  |  |
|  | 7 | " |  | aud-intrphn |  |  |
|  | 8 | " |  | del-A/C headng |  |  |
|  | 9 | " |  | del-nav flag |  |  |
|  | 10 vid sig | ant rcv |  | aud |  |  |
|  | 11 strb sig | " |  | aud,del-stick |  |  |
|  | 12 dig sig | " |  | aud |  |  |
| Radar: | 1 rdr | prx sw | RE | lose antiskid | fil,bnd,shld | inc RF |
|  | 2 HF tx | cmptr |  | ind-lts |  | level |
| Power qualty: | 1 powerline | cmptr | 26v | del cmptr | fil,bnd,shld |  |
|  | 2 | " | 115v | dis cmptr |  |  |

### 2.6.3. Corrective Action and Modeling

A comprehensive study of troubleshooting is needed before accurate corrections to the aircraft system specifications or the RTCA DO-160 equipment specification can be recommended. Documented, statistical groupings of troubleshooting experience concerning historical EMI characteristics and cost factors do not exist, but one might postulate some possible categories and hypothetical percentages as shown in the accompanying pie charts (figure 2.6-2).

A study of categories such as these might reveal that analysis and modeling of analog/audio circuit susceptibility is most beneficial, or possibly better models of aircraft wire coupling might help, or even modeling and documenting of the most popular fixes.

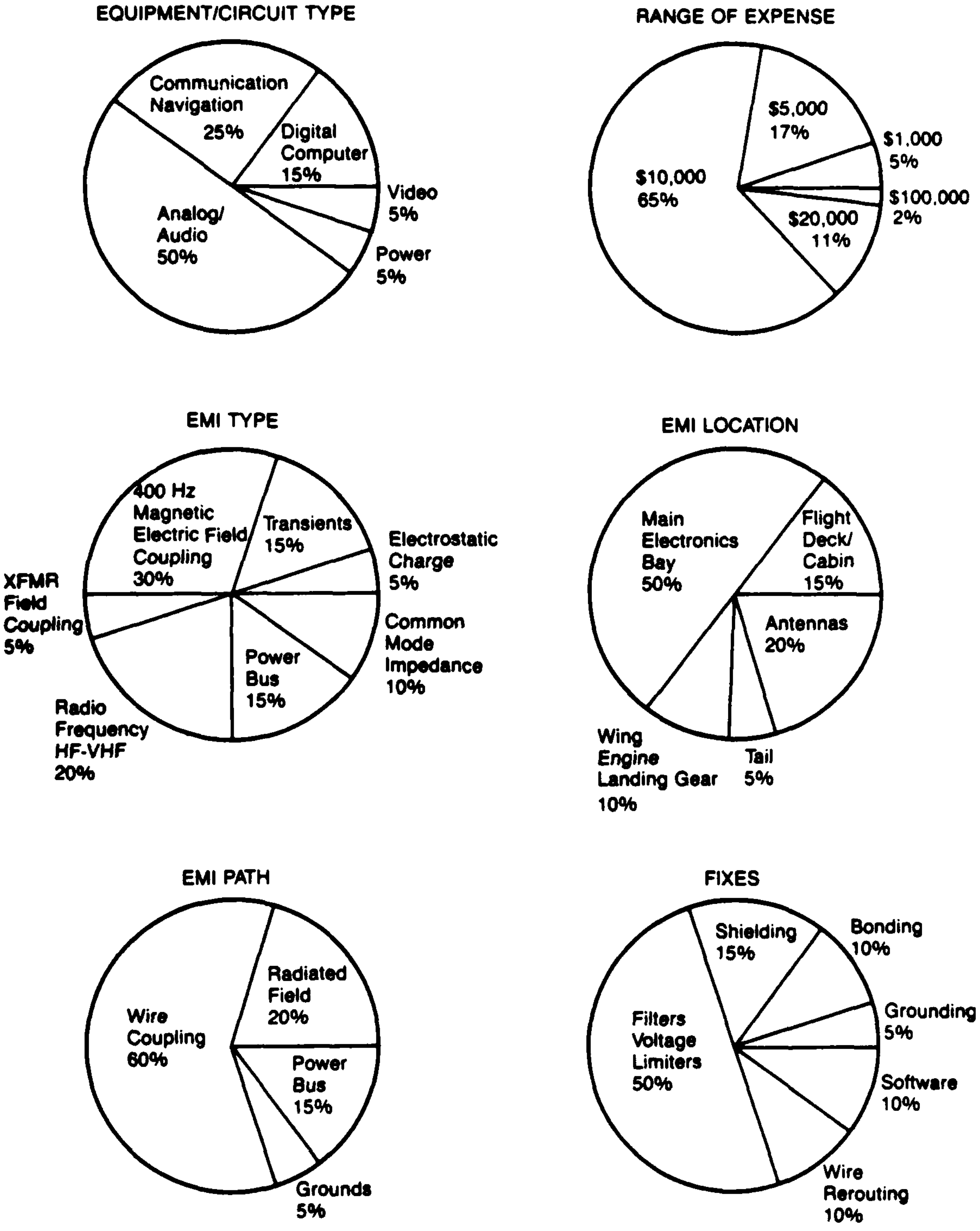


FIGURE 2.6-2. POSTULATED HALLMARKS OF VARIANCES

# 3. AVIONICS THRESHOLDS AND PROTECTION

## 3.1. Hardware Tolerance

Recognizing the conditions of proper interface wiring design, circuit protection, and the contributions of aircraft structural shielding protection is of course important in a "top-down" electromagnetic compatibility design of an aircraft, but these recognitions must also be tied closely to a knowledge of the noise tolerances and noise thresholds of transistors, micro-circuits, and logic. The lines can be drawn: environment, protection, threshold.

Airplane environmental noise voltages flourish far above the transistor and micro-circuit thresholds of damage, upset, or offset, which means that micro-circuits demand protection in every case. Transistor-Transistor-Logic (TTL) gates and microprocessors do not have even a modest tolerance to the run-of-the-mill aircraft noise types, such as electrostatic pulses, lightning induced transients, inductive switching transients, or even some high-energy radio frequency signals.

A TTL logic gate will "change state" at a threshold of about 800 mV when radio frequencies are injected starting at low frequencies and on up into the megahertz range, but in the tens to hundreds of megahertz the threshold rises to greater than 5V before upset occurs. Figure 3.1-1 maps that threshold. Whereas a gate will operate or change state at 800 mV it may be damaged if subjected to much greater than 10V at low frequencies and can usually survive about 100V transients that are of microsecond or nanosecond duration depending on thermal dissipation. As shown in the figure, a transistor or semiconductor "PN" junction will detect power levels as low as 100 $\mu$W under certain conditions.

Microprocessor chips are high density and high speed. Microprocessor circuits may be upset, change state, or change performance when signals with noise power levels down to 10 $\mu$W are injected on signal, address, or clock lines. As frequency is increased beyond the operational range of a microprocessor, the power required to cause upset and damage increases. These levels change with conditions such as loading, circuit geometry, radio frequency paths, and sometimes software design. Operational factors such as address or memory or timing or process changes affect the definition of upset. Under the onslaught of steady state, low-frequency signals, microcircuits can be damaged at power amplitudes of less than 1W, but high frequencies or fast narrow pulses require much higher wattage levels - ten to hundreds of watts.

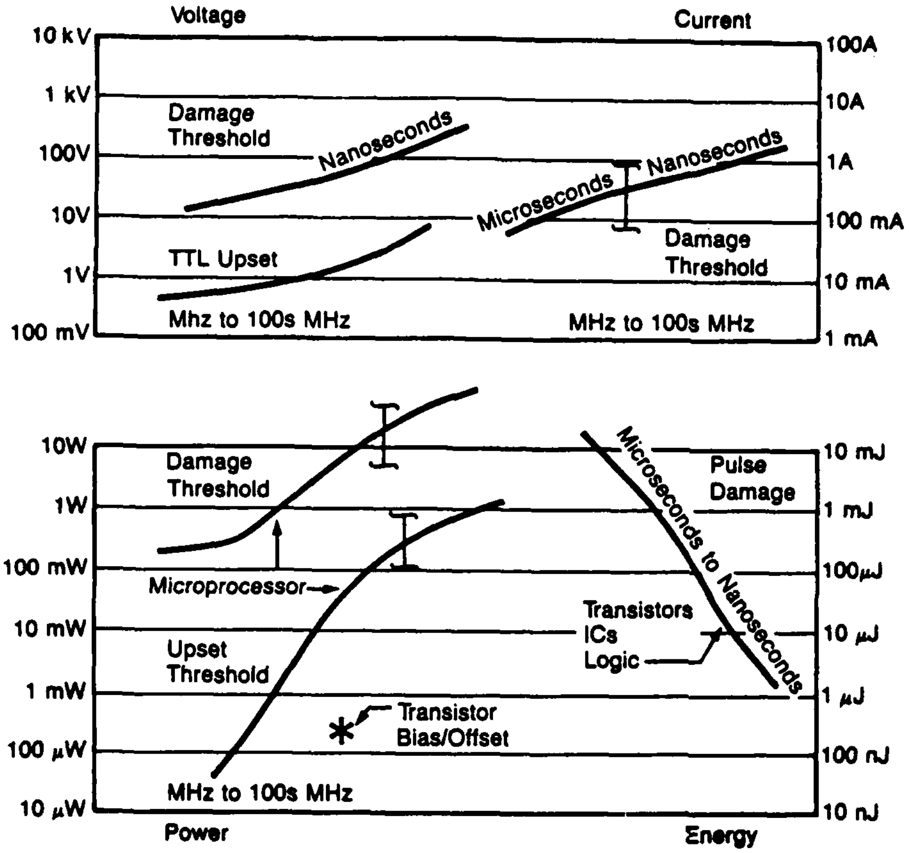
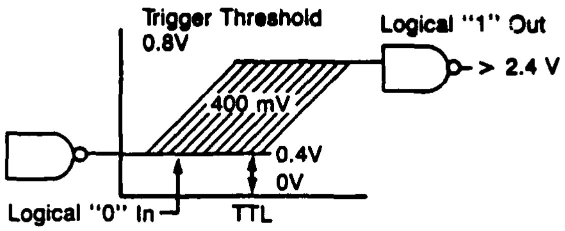


FIGURE 3.1-1. MICROCIRCUIT TOLERANCE



| | Transistor-Transistor Logic TTL | Emitted Coupled Logic ECL | High-Threshold Logic HTL | Complementary Metal Oxide Logic CMOS |
|---|---|---|---|---|
| Average | 1.2V | 100 mV | 7.5V | 2.2V |
| Minimum | 400 mV | — | 5V | 1.5V |

FIGURE 3.1-2. NOISE MARGIN

Individual pulses, measured by their energy content, require anywhere from 10 mJ to 1 μJ to cause damage as shown in figure 3.1-1. Pulse durations are microseconds to nanoseconds  Awareness of these levels is important when designing the shielding for the aircraft or avionics wiring to protect against HF transients or resonances.

Shielding protection or voltage limiting must be provided to reduce transient noise signals below the damage threshold. Protection must also be designed to keep continuous wave radio frequencies below the TTL or integrated circuit operational thresholds (figure 3.1-2). Software can be designed to correct for random, nonrepetitious transients.

Extensive effort in testing, modeling, measuring, and graphing operational upset and damage levels has been documented in the industry. Minimum and maximum spreads are available. Voltage damage amplitudes may vary by a factor of two or three, say from 100V to 300V from one manufacturer to another, or from one lot to another. The threshold of operation may vary from 800 mV to 1.5V from one transistor to another. Damage thresholds change by a factor of ten or more with the number of transient pulses and the rate of applying them. The spreads and averages are interesting in the study of susceptibilities, but at the bottom line is this: protection must be built in to account for the minimums - for example, 100V for transient damage, 800 mV or less for TTL gate state change, and 10 μW for microcircuit performance alteration. It is necessary to constrain radio frequency power and stored transient energy access to avionics by diverting and/or blocking the noise with balanced circuits, filters, or shields on every input-output interface circuit.

When two conductors are spaced 100 mils (2.5 mm, 2500 μm) apart, and the voltage between them is slowly increased, an arc will start (at sea level, atmospheric pressure) and establish itself at around 2000V or 3000V. If there are only 20 mils of spacing (0.5 mm, 500 μm) between the conductors, the arc will start at 1000V. Circuit card conductors have these close spacings. So it is easy to understand when microcircuits, chips, and thin-film devices with substrate circuit separations of a few microns fail at 100V.

## 3.2. EMI and Software

It is difficult to know where to start in the treatment of electromagnetic interference relative to software in an aircraft context. What is special about an aircraft? How does aircraft electromagnetic interference uniquely relate to software?

Not by component failure or damage: damage may appear anywhere, anytime - broken parts - vibration - faults - mishandling.

Not by errors or deficiencies in software itself: this is the purview of the software designer; he must compensate for these regardless of aircraft electromagnetic interference. And also, not especially by the internally generated noise from power and switching regulators, or clocks and data lines: noise sources found in any electronic package.

The aircraft associated electromagnetic interference arises from power line 400 Hz, radio frequencies, electrical transients, and power bus momentary interruptions. They are very different in their characteristics, their occurrence, and their threat of upset. Two of these noise threats must be eliminated from software concerns right away.

First, 400 Hz is simply 400 cycles per second of a noise voltage from the power line imposed on a neighboring circuit. Cycle duration time is 2.5 ms; with zero to peak being 625 us; the positive risetime repeats every 2.5 ms. If a balanced circuit is slightly unbalanced and responsive for any reason, the 400 Hz will trigger operation of the balanced circuit continually or, much worse, in an intermittent fashion. If there is an error or disorder from 400 Hz, then there has been an error in the original design that must be fixed. Four-hundred Hertz must be controlled and kept out of interface circuits.

And second, radio frequencies can also be eliminated from software concerns. Aircraft wiring cannot be allowed in a radio frequency field stronger than the original design specification. If a digital circuit sees an overlay of an unwanted radio frequency (not damaging, but causing loss of data), the software will not be able to correct upset. The radio frequency environment must be known, documented, and immunity designed in to the interface circuits. Transmitter radio frequency noise and digital data are in the same frequency range, the most important being HF-VHF, 1 to 300 MHz.

Transients are the problem. Electrical transients have existed in the past, they exist today, and will continue to exist on the airplane as well as in the laboratory. Electrostatic discharge, lightning, or powerline inductive switching transients are usually of large magnitude (hundreds to thousands of volts). The amplitudes are reduced below circuit damage level (100V; a few amps) by design; but transients are sometimes not totally rejected, and they result in short-term destruction of data words. It is the responsibility of the EMC engineer to supply threat transient levels and repetition rates to hardware/software designers to assure proper programming of fault tolerance and detection. What, then, are the time characteristics of transients relative to data words that the software designer must know to override noise or make software tolerant to noise?

Some inductive switching transients have ringing frequencies of 10 MHz recurring at a 1-MHz repetition rate and lasting for around 1000 μs (figure 3.2-1). During test, the transient is repeated every two seconds. (DO-160 specifies 8-10 pulses per second for 10 seconds.) A 12-kHz, ARINC 429 signal has a bit width of 80 μs, and the 32-bit word has a duration of 256 μs. A 1000 μs, inductive switching transient can decimate a 256 μs data word.

An electrostatic discharge, on the other hand, is a very fast 100-ns event (figure 3.2-1) and probably does not recur until after sufficient time, possibly 4 or 5 sec, to recharge the object originally collecting the charge. This transient might only affect one bit.

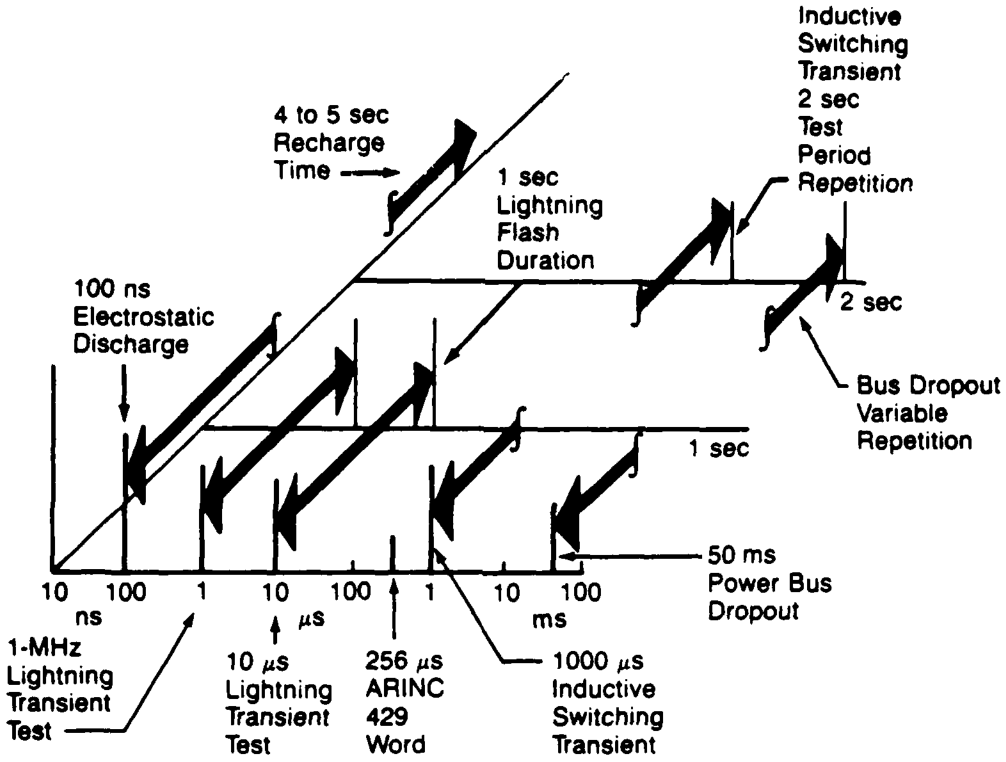

Inductive Switching Transient 2 sec Test Period Repetition
4 to 5 sec Recharge Time
1 sec Lightning Flash Duration
100 ns Electrostatic Discharge
2 sec
Bus Dropout Variable Repetition
1 sec
50 ms Power Bus Dropout
10
ns
100
1
10
μs
100
1
10
100
ms
1-MHz Lightning Transient Test
10 μs Lightning Transient Test
256 μs ARINC 429 Word
1000 μs Inductive Switching Transient

FIGURE 3.2-1. TRANSIENT EVENTS

Lightning transients have low frequencies, 10 μs or longer, and ringing high frequencies, for instance at 1 MHz, 3 MHz, and 7 MHz, set up by the electrical resonant lengths of an aircraft and damped out in a few microseconds; but then they may recur again and again under multiple strokes of a total lightning flash lasting for possibly one second (figure 3.2-1). A lightning flash might result in disorder in a number of words.

Of important concern is the momentary interruption of the power bus, referred to as a "bus switching" or "dropout" transient, where power drops or decays to zero for up to 50 ms (figure 3.2-1) when the power supply is transferred from ground power to engine power or from one engine generator to another. (DO-160 has a test requirement of a 200 ms interrupt for ac equipment, and a 1-second interrupt for dc equipment.) Software control may be required to ensure a graceful shutdown, proper data storage, or even continued processing.

So the software designer institutes techniques to control equipment operation, override errors, and make software tolerant to noise when transients and power shutdown occur.

There are a number of methods employed for data correction and resetting, such as:

- Microprocessor reset to initial state ("backward")
- Microprocessor forced to known state ("forward")
- Functionally equivalent, but dissimilar backup system
- Data word repetition or redundant data supply

There are also a number of means of detecting errors of data, flow, or hardware operation, such as:

For data checks -

- Read after write on output data line
- Data bus activity, reasonableness check, data averaging
- Bits per word, parity, status bits
- Check sums: averages, spreads, maximums, minimums

For flow checks -

- Out of sequence, out of loop
- Excess or deficient time
- Event record of activity with respect to total program execution ("state activity")

It may be postulated that the aircraft has five layers of protection: (1) structure shielding, (2) circuit shielding, (3) balanced circuit, (4) voltage/current limiting, and (5) software. Software is the last line of defense.

## 3.3. Digital and Discrete Circuits

### 3.3.1. ARINC 429 Drivers and Receivers

The ARINC 429 bus, a digital transmission interface system, fans out from the main equipment bay to the flight deck and to external sections in the wing, engine, or empennage. With two or more 429 circuits per unit, there could be two- to three-hundred individual buses. They may reach 100 ft (30m) in length, and are routed in bundles where they encounter transients, radio frequencies, and power line noise. The ARINC 429 "MARK 33" Digital Information Transfer System (DITS) offers immunity to noise by using a well designed combination of a balanced circuit, a relatively high-trigger threshold, a "high-resistance" input, and finally, wire braid shielding. Parity, status bit, and "bits per word" software checks help to extend protection even further.

The output signal of the 429 transmitter measures at the high level, 10 ±1V "line-to-line" and at the low level, 0 ±0.5V. At the other end of the line, the receiver must operate with an input signal at a high level of 6.5V to 13V and be at a low below 2.5V. The margin from 2.5V to 6.5V is undefined.

The trigger threshold of operation, therefore, can be 2.5V.

The transmitter driver output resistance is 70Ω to 80Ω "line-to-line" and the receiver input resistance is 12 KΩ or greater in each line so that there is at least 12 KΩ resistance in the circuit from transmitter to receiver. That is an important resistance for protection against transients. The high resistance provides immunity. Just ignoring the shield for a moment, if a 600V transient occurs on the wire and appears at the 12-KΩ input, the resulting current amounts to only 50 mA, a very low "transient" current and not enough energy for damage.

The ARINC specification does not define the circuit ground or case ground. For shields, the specification states that: "The circuit should be twisted pair shielded from data source to sink with the shield grounded at both ends at an aircraft ground close to the rack connector." Shield tie length is not defined. The 429 system has been subjected to the RTCA DO-160 electromagnetic interference tests and passed. Three factors in implementing this digital bus design demand extra effort in manufacture to ensure quality: (1) electrical tolerances of components (avionics supplier responsibility), (2) shield tie to ground (airframe manufacturer and supplier), and (3) case ground (airframe manufacturer and supplier). Future digital buses may have similar noise characteristics and rejection capabilities.

The 429 is a balanced circuit, and balanced circuits are important; the installation of shields is also important, but grounding decides effectiveness of receiver immunity: the grounding of the box, the grounding of the circuit, and the grounding of the shields.

### 3.3.2. Circuit and Shield Grounds

Noise on a single wire in space with no connection to a ground plane cannot be measured, and no current flows for an "electrically short" wire.

Connect one end to a ground plane and an induced noise voltage in the wire of 1V can be measured at the other end, the ungrounded end. This is a single wire over ground (figure 3.3-1a) and is the technique used to install the "discrete" circuits on the aircraft. It is susceptible over the entire frequency range.

If the ungrounded end is left unconnected, practically no current flows and no energy is dissipated. That's an incredibly significant fact when analyzing for protection against damage. If no current flows, components cannot be damaged. Where circuits are exposed to high-level transients on the wing, isolate them at one end if possible.

Now, two wires over a ground plane with resistors between them at each end to form a circuit and one end connected to ground, say the source end, sets up the same condition - all the voltage will be measured at the load end relative to ground, with practically no voltage across the load resistor at low frequencies.

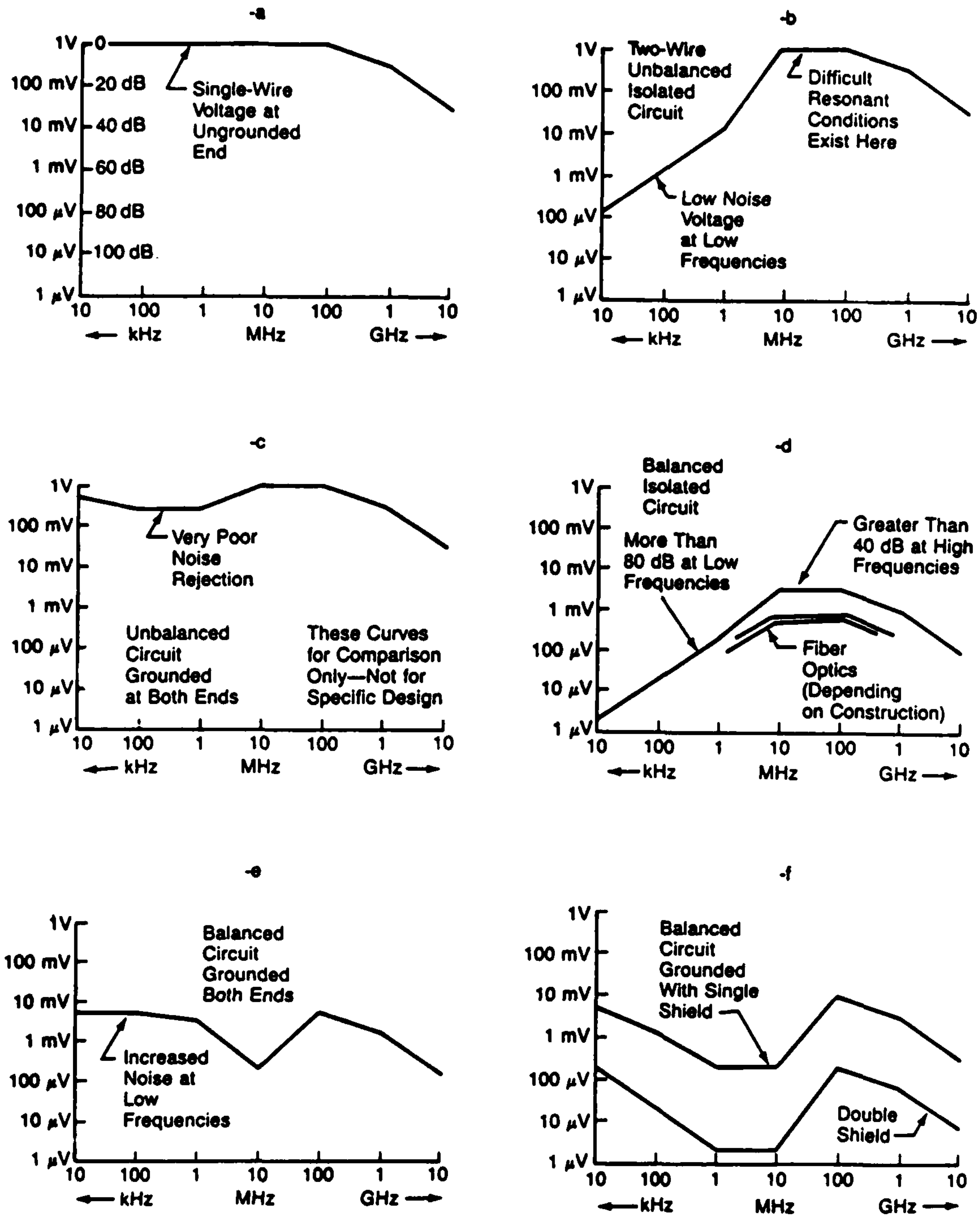


FIGURE 3.3-1. CIRCUIT NOISE REJECTION (A B C D E F)

This is a two-wire, unbalanced circuit (figure 3.3-1b). At the higher frequencies, resonance exists and voltages appear.

A two-wire, unbalanced circuit grounded at both ends, source and load, offers practically no noise rejection, maybe 10 dB or so (figure 3.3-1c). The noise rejection is lost at low frequencies.

Make the circuit a balanced circuit, as the 429 is, and it can establish more than 40 dB of noise rejection for "differential mode" line-to-line voltages (figure 3.3-1d) at the higher frequencies. The line-to-ground noise, called "common mode," remains the same as the unbalanced circuit.

In an aircraft installation, it is optional whether or not the balanced circuit is grounded. Grounding loses some of the low frequency protection (figure 3.3-1e). The balanced, isolated design can offer 80 to 100 dB at low frequencies, just about equivalent to fiber optics or transformer isolation under practical installation conditions.

Figure 3.3-1f shows a comparison of one shield (like 429) and two shields grounded at both ends with the circuit and equipment case grounded. If either the circuit or case were lifted from ground, the circuit would have much more low frequency isolation and protection.

A balanced circuit (either grounded or isolated) that is double shielded with shields tied to the case connector and the base surface of the enclosure case grounded is almost always the best. The circuit can be isolated with a transformer, optical device, or fiber optics. This is the optimum practical design for low and high frequencies.

### 3.3.3. Discretes

A "discrete" circuit is designed and installed to indicate events, such as on or off, engaged or open. Sometimes it is constructed using a single wire (figure 3.3-1a) from the electronics bay out to a unit on the wing where a switch, to provide indication, grounds it to structure using the structure as the return. Their thresholds are high and, therefore, radio frequency noise is usually not a problem. But these circuits can be hit with the full force of transients and need to be protected with shielding, voltage or current limiting, or increased power ratings.

## 3.4. Equipment/Wiring Isolation and Separation

### 3.4.1. Quality of Wiring Design

If there are no wires, there is no electromagnetic interference. Wiring takes on different characters in its role as a conductor of signals. It is a signal conductor, driver to receiver. It acts as a transmitting radiating antenna or a very efficient receiving antenna; it is a party in transformer action to participate in voltage-current-energy transfer when in a cable bundle; and it also acts as an intermediary or a transfer agent to import electrical energy, then retransfer that energy to other wiring - sometimes called secondary coupling.

The wiring design is a fabric, a multi-weave electrical mosaic. There is a mosaic of conditions: wire size, grounding, returns, shields, shield ties, separation, and wire length. There is a mosaic of properties: metals, dielectrics, resistance, inductance, capacitance, impedance, and nonlinear effects. Careful analysis and development of the design will bring about an acceptable level of electromagnetic interference and a cost-effective electromagnetic compatibility.

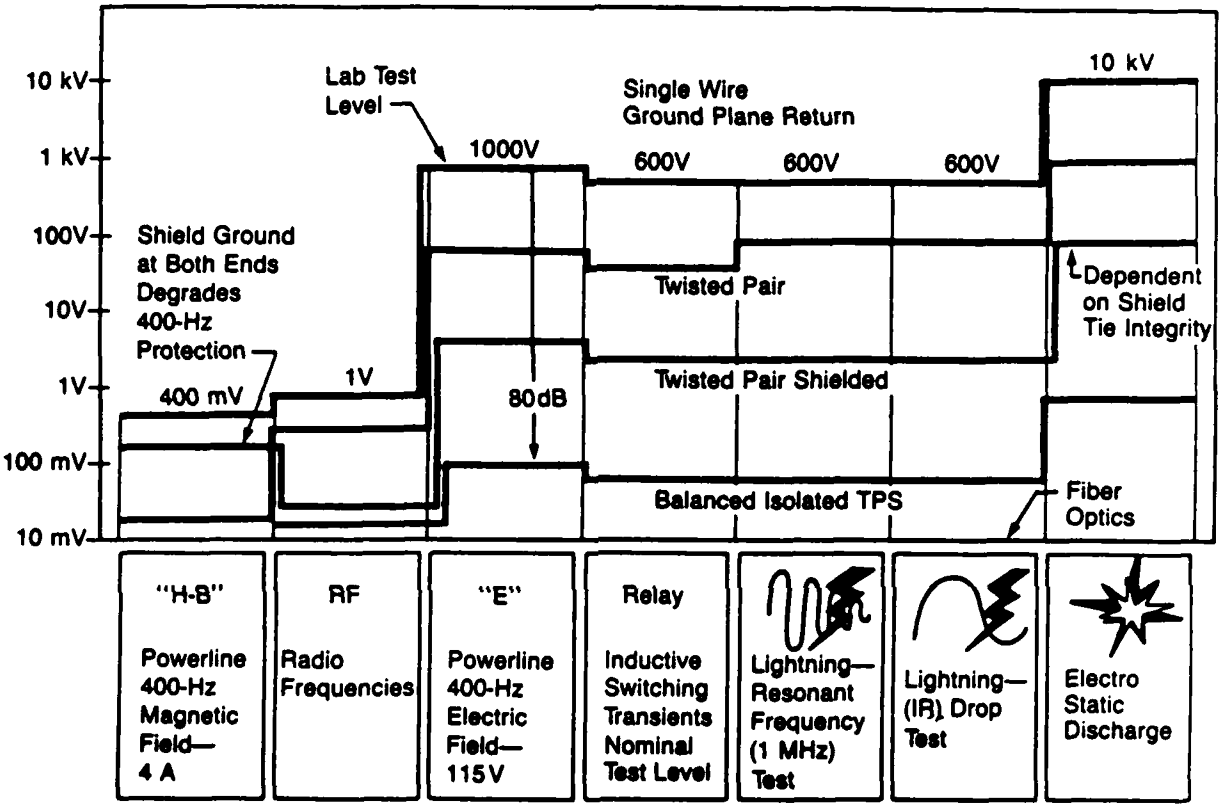


FIGURE 3.4-1. CIRCUIT RESPONSE TO EMI

The complexities of the mosaic could be largely dispelled through the simple use of a twisted-pair-shielded (or coax), balanced-isolated circuit design that reduces noise, and sustains signal quality. See in figure 3.4-1 how the twisted pair, shielded, balanced circuit has reduced noise to an acceptable level. This design provides a winning combination. It is the king of avionic interface design, boasting a possible noise rejection of 80 dB (10,000 times) and finding widespread use in digital communication or control circuits where stability, quality, and signal fidelity guarantee performance and confidence. Figure 3.4-1 was constructed to illustrate the general levels of improvement for comparison, but is not appropriate to be used or adapted to specific designs.

The building blocks to signal wiring quality are threefold: twisted pair for minimum magnetic field induction, down by 60 dB; shield for minimum electric fields, down by 30 dB or more; and balanced isolated design for a minimum common impedance, down by 40 dB. For future aircraft, it will be necessary to accurately model types of circuits on an aircraft to understand the induced noise levels and assure desired signal quality. Determination of the actual voltage, current, power, or energy on the wire circuit is the goal. Current and power become important when designing the rating or sizing of circuit protection.

There is no easy answer to avionic interface wiring design. Interface circuits can be built (by careful engineering evaluation, assessment, and construction) to offer optimum circuit compatibility through four fundamental approaches:

- Equipment and wiring location/grouping/organization design.

- Connector choice and wiring assignment.

- Return current rule.

- Coupling and modeling analysis.

Definition of the total circuit is required: the driver, the wiring, the receiver, operating frequency, and intercircuit connections. The following tasks are applicable: identification of all identical circuits; identification of all common circuits, common returns, every ground connection, capacitor, or resistor connection; determination of output and input impedances, balanced and unbalanced impedances to ground. A check of other current paths that are not intentionally designed is often appropriate, such as, circuit paths from ground wires through mutual capacitances (leakage capacitance), through other ground conductors or transformers, shields, and circuit card grounds.

Identical or common circuits are best assigned to the same connector. Circuit currents should exit and return in the same connector. Low-frequency signals, less than 1 kHz, may return in a well-signed aluminum or copper grounding structure where transmission line design techniques are not necessary.

These rules are constructive:

- Separate power and signal (if power must be in the same connector as signal, separate power and signal by ground pins).

- Separate families of circuits in individual connectors by frequency: audio, digital, pulse width modulation (PWM), video.

- Position wires for shortest practical route to other equipment.

- Assign connectors for optimum wire routing to other equipment.

Current paths returning in structure are designed to follow immediately adjacent to the cable (an image path). Currents should not be forced to take a wide path through distant connectors and structure. This is sometimes called the return current rule.

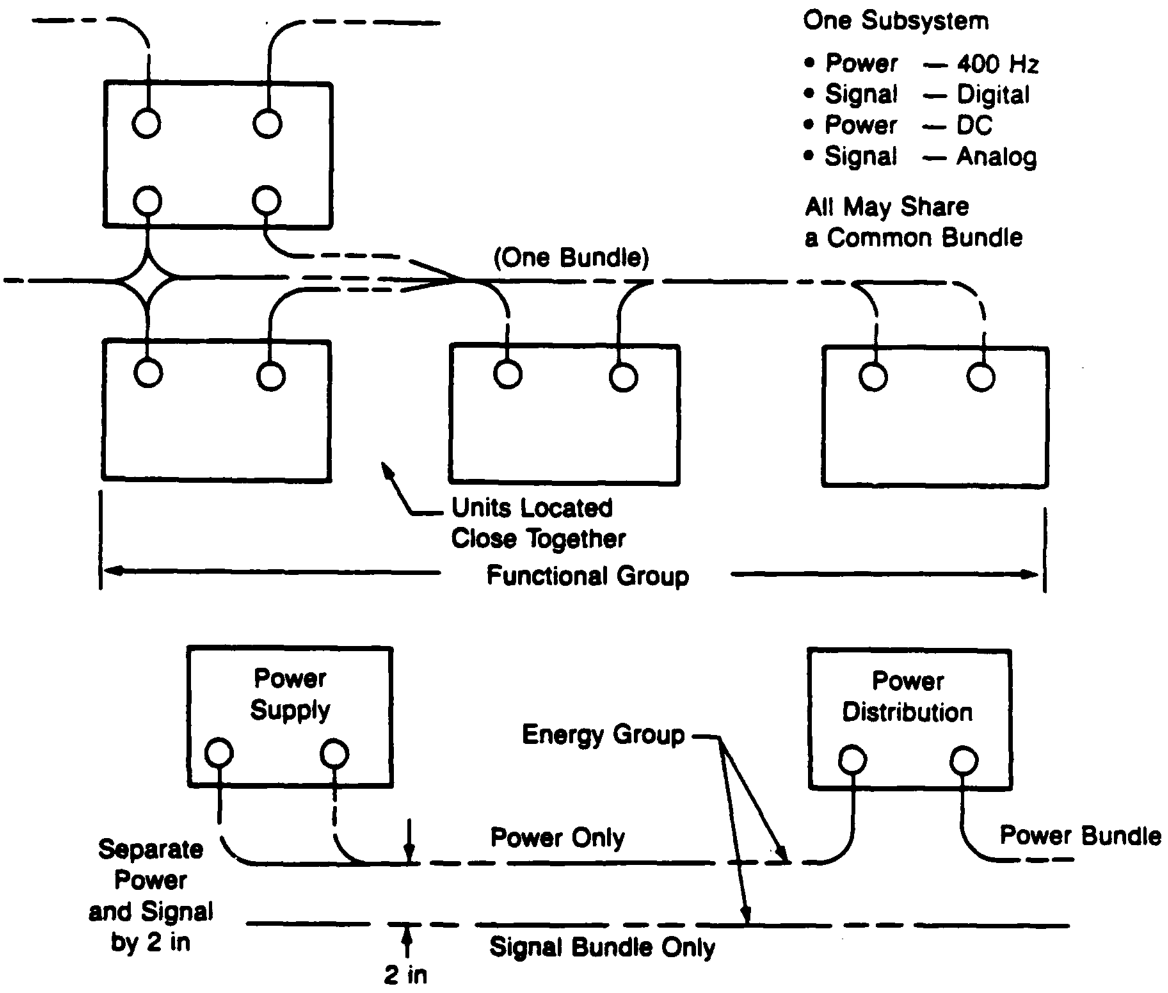


FIGURE 3.4-2. WIRING CATEGORIES

A simple way to achieve electromagnetic compatibility in wiring or in equipment is by functional or subsystem grouping (figure 3.4-2) - that is, keeping units or equipment of the same subsystem close together. An early definition and visibility of the system design, configuration, and function must be obtained. Equipment and subsystems and their locations must be known:

- Primary power, secondary power, distribution boxes, heavy switching (solenoids), lighting.

- Electronic flight control, electronic flight instrumentation, engine electronic controllers.

- Navigation, VOR, ILS, and DME.

- Radio transmitter/receivers, HF, VHF.

An early developmental wiring mockup is a requirement for good wiring design. The best design is grouping the subsystems close together in an in-line design. Generator to receiver, input to output, and source to load. Individual connectors can be dedicated with common groups of circuits. Functional grouping can often be extended in the aircraft between units that are widely separated. Here, engineering judgment and analysis is important. Where functional grouping is used, bundles are more easily separated to comply with redundancy and safety requirements or a separation of wiring to protect against physical damage to redundant critical equipment such as engine-mounted electronic controllers.

On long wire runs, functional grouping may result in excessive coupling between noisy lines and susceptible or sensitive lines. Where space is available, it is recommended that wiring be separated by "signal/energy" categories as follows:

- Ac feeder power bus; large ac control circuits; heavy current dc or secondary ac switching circuits valves, motor, or actuator drives; large inductive loads.

- Standard 115V and 28V power; signal circuits and regulated power circuits.

- Low-level, sensitive circuits such as audio, analog, dc reference, or dc secondary power.

- High-power radio frequency circuits (coax) or high-level pulse width modulated (PWM) circuits.

Wire separation is not the best way to reduce noise between circuits, but it is often necessary. Separation is very effective when used for isolation, redundancy, and safety (figure 3.4-3). Independent computer controls, instruments, power sources, or standby instrumentation are isolated to increase reliability. Left and right engine power lines and circuits, as well as engine indication signals, are separated and isolated. Communication, EICAS systems, ILS, LRRA, DME, and computer control devices, FMC, ADC, are separated and isolated. Primary controls (for example, roll, pitch, yaw, and stabilizer or spoiler controls as well as position sensors) are isolated.

### 3.4.2. Power and Energy Levels

A twisted pair shielded, balanced, isolated circuit, properly designed into the system as an interface circuit, minimizes the possibilities of noise-induced damage and establishes a basic high-quality design. But not all circuits are balanced and use a return wire; some interface circuits on the airplane have a ground return (structure return).

It is helpful and instructive in the initial design stage of a program to have a concept of the magnitudes of not only the noise voltage amplitudes but also the power and energy levels of radio frequency signals, 400-Hz power, and

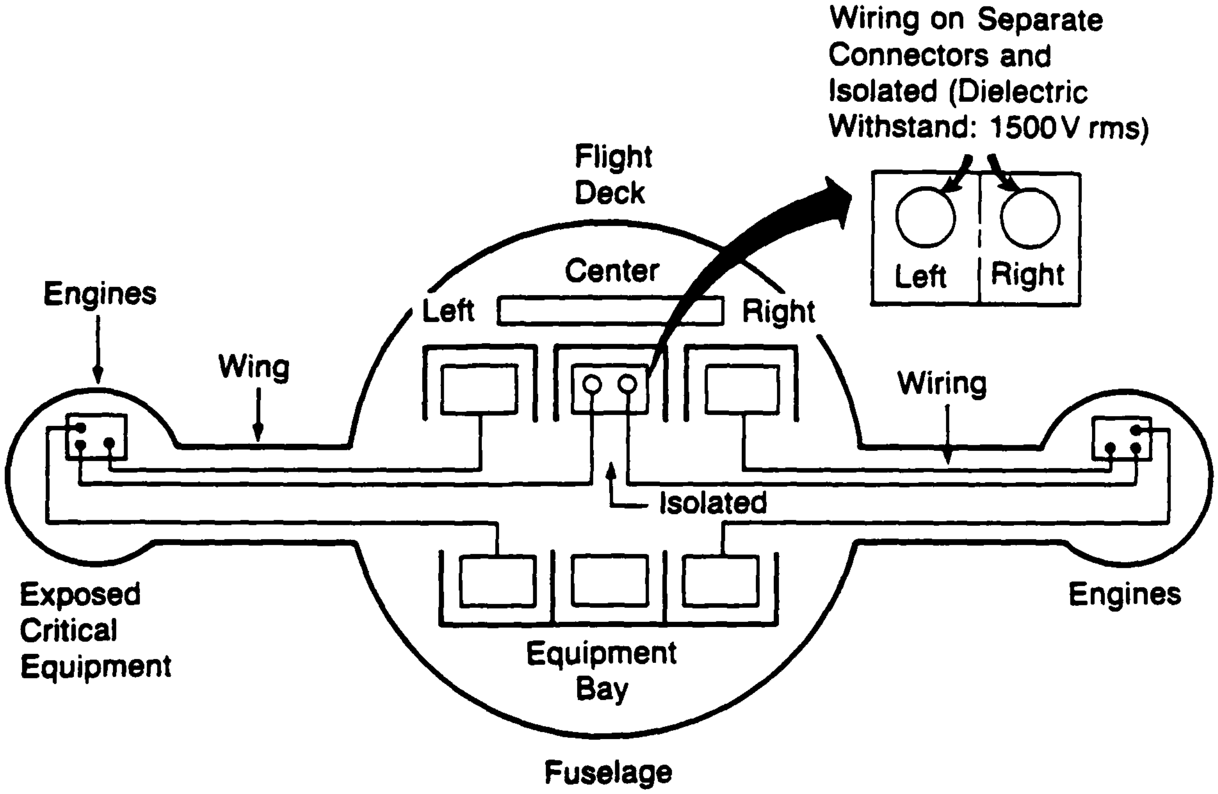

Wiring on Separate Connectors and Isolated (Dielectric Withstand: 1500V rms)
Left
Right
Flight Deck
Center
Left
Right
Engines
Wing
Wiring
Isolated
Exposed Critical Equipment
Engines
Equipment Bay
Fuselage

FIGURE 3.4-3. CRITICAL CIRCUITS WIRE SEPARATION

transient noise that can be imposed on a circuit which uses structure as the return path. It is important to analyze and define the power level (for continuous signals) and the energy levels (for transients).

One way to do this is by looking at selected electromagnetic interference laboratory test levels (figure 3.4-5). The test levels shown here are the avionic equipment test levels seen by equipment itself and are not the actual environmental magnitudes that may exist on the aircraft that the airframe manufacturer must consider, such as, higher levels of radio frequency signals or lightning transients.

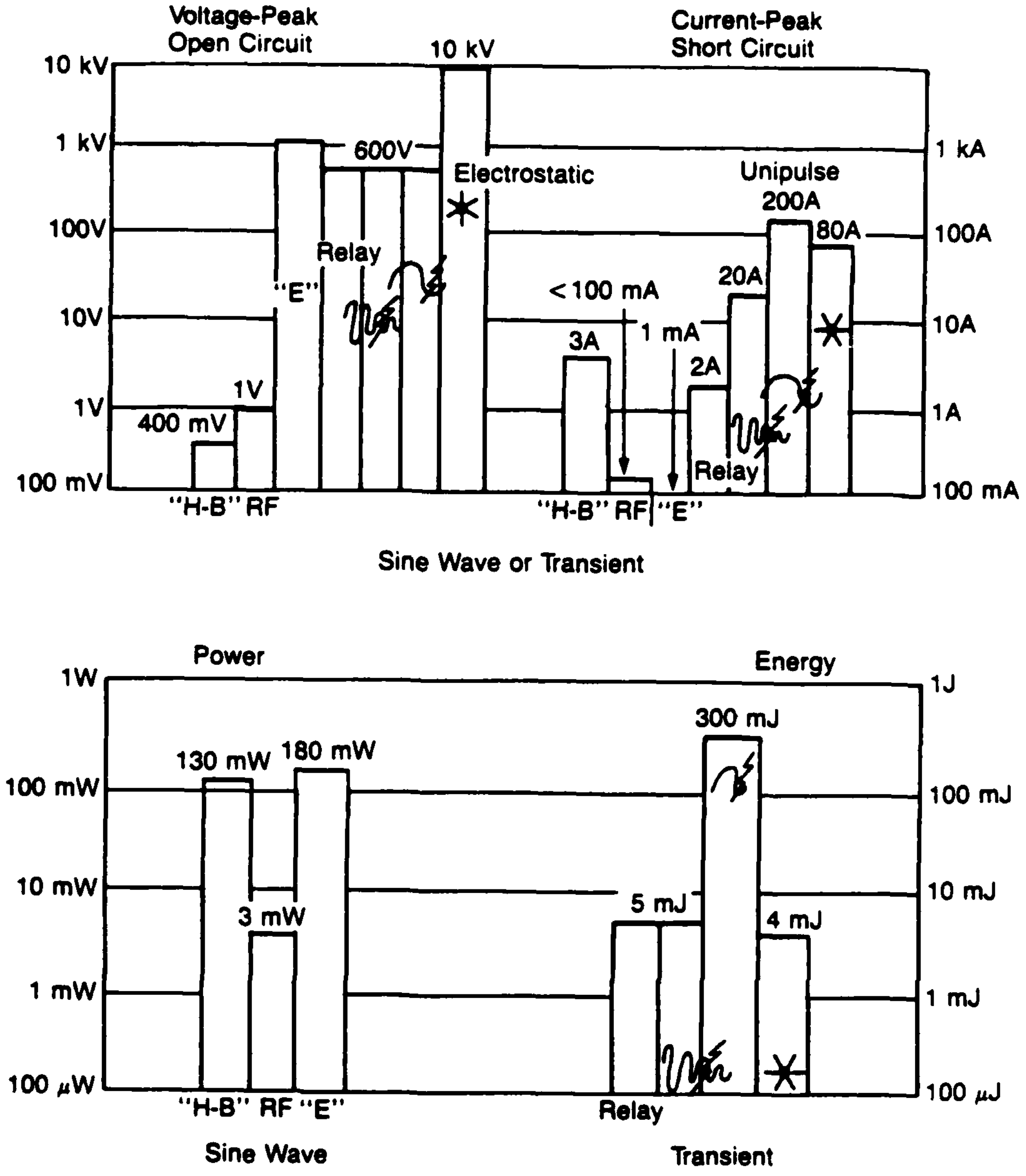


FIGURE 3.4-4. SELECTED EMI LEVELS

Seven electromagnetic interference types can be listed for the purposes of identifying, summarizing, and comparing their voltage-current-energy and power profiles. In these selected laboratory test setups, certain circuit parameters and conditions must be arbitrarily defined. Therefore, the levels shown in the figure are illustrative and helpful for making comparisons, but are not appropriate for detail design conditions and must not be used or adapted to specific designs. The electrostatic discharge test is not an industry standard test level and is shown here for comparison to the other forms of noise. The amplitude is arbitrarily set at 10 kV, a nominal value out of an actual range of about 3 kV to 50 kV. Referring to figures 3.4-4 and 3.4-5:

- The radio frequency test induces a low voltage, 1V and a low current, approximately 100 mA, on a single wire that has a ground plane return. Observe on the bar chart the radio frequency voltage level of 1V and then the radio frequency current level of less than 100 mA. Now move down to the power bar chart and see the radio frequency power level of 3 mW. The power level is shown because it is a continuous signal. This test is performed in the laboratory using a current probe to induce the radio frequency voltage measured as an open circuit voltage (figure 3.4-5). The test level here is chosen as 1V (in the HF-VHF range) induced into a wire that is 5m (15 ft) long. The calculated current is the short circuit current and the load resistance is adjusted for maximum power.

  These radio frequency signal products come from aircraft microprocessor clock and switching regulator stray noise signals as well as HF-VHF aircraft communication, HF-VHF television, and FM radio broadcast transmitters. Radio frequency carries with it the ability to sneak through avionics internal circuit capacitors or diodes connected to power supplies, and on a circuit card it will pass from circuit trace to trace. The radio frequencies are not damaging, but they can alter circuit operation and performance.

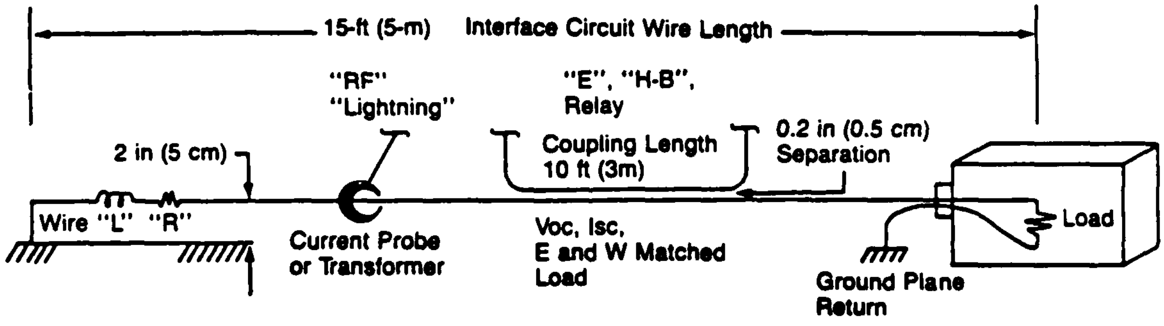


FIGURE 3.4-5. LABORATORY TEST SETUP

- The power line 400-Hz magnetic field, designated as "H-B" on the chart, delivers a low-frequency effect into analog circuits or operational amplifiers. Mark on the chart how the magnetic field might impose 400 mV with a power of 130 mW.

  For this laboratory setup, a 40A current is coupled into a 3m (10 ft) section of wire, with a 0.5-cm (0.2-inch) separation, and positioned 5-cm (2-inch) above the ground plane. This simulates a 4A, 30-m (100A-ft) maximum coupling condition on an aircraft. The power is calculated for a load resistance equal to the 5-m wire resistance.

- The power line 400-Hz electric field ("E") also delivers a low-frequency effect into analog circuits or operational amplifiers. See how the electric field ("E") is about 1000V, but note the extremely low current, less than 1 mA (off the chart). The power level is low but easily large enough for upset or alteration of equipment performance. Notice here that the power line test is performed at 10 times the 115V line level, or 1150V, in order to use a 10-ft coupling length. This simulates a 115V 100-ft maximum coupling condition on an aircraft.

- The electrical switching transient test (relay induced transient) may impose voltages of 600V or higher with currents of just a few amps and energies in the range of millijoules - large enough to damage sensitive solid state devices. For this test, the electrical parameters were estimated with the following values chosen: 600V peak-to-peak voltage; 2A current; a 1-MHz damped sine wave, repeated 1000 times to simulate a transient of 1-ms total duration. This is an arbitrary electrical switching transient for illustration only.

- The 1-MHz lightning-induced transient (designated by the damped sine on the bar chart) is a damped cosinusoid, has a set 600V amplitude, is transformer-induced into the wire, has an initial fast risetime of about 100 ns (3 MHz), and is to simulate lightning resonance on the aircraft. The induced current is high but the energy is fairly low.

- The so-called "ground potential test" (designated by the pulse waveform on the bar chart) is a 600V 10$\mu$s unipulse or "double exponential" waveform to simulate a controlled lightning induced current transient in structure. Observe on the figure the dramatically higher current, 200A, and much higher energy of the unipulse. The unipulse is a very powerful noise source. It carries a considerable amount of energy and can easily damage and destroy electronic components. A balanced circuit design or substantial protection is needed to divert or block this transient. The test setup is different from that shown in the figure. The 600V waveform from the transient source is pre-established on a 5Ω load, then the voltage is applied with a "source" transformer connected between ground and the avionics case, housing (and any signal return) where the resulting waveform will vary depending on avionic equipment circuit loading and wiring design. Any circuit using structure as return will receive the full impact of this transient.

- The profile of the electrostatic discharge transient (designated by the "star" on the bar chart) shows an exceedingly high-voltage pulse of 10 kV, which is capable of causing dielectric breakdown of insulation rather than the usual condition of thermal burnout of a semiconductor or microcircuit. The short circuit current can be high but the width or duration of the pulse is so narrow or short that it results in a low energy level. The application is different from that shown in the test setup figure. The transient is applied directly to the circuit wire or connector pin. These electrical parameters apply: 150-pF, 50Ω source through a 1-$\mu$H, 1-m wire to a simulated 50Ω load for maximum power transfer.

### 3.4.3. EMC Quality in Maintenance

Structural shielding, wire shielding, and interface circuit protection must be maintained through the life of the aircraft. Here are some of the most important items:

- Keep the controlled wire routing and the wire separation design intact. The original design of wiring is formulated to ensure that faults will not propagate, that critical functions are redundant, and that electrically noisy circuits are separated from vulnerable circuits.

- Concentrate on maintaining short shield ties to the structure or to "line replaceable unit" (LRU) box if structure is graphite-epoxy. Shield ties or "pigtails" do not usually receive the attention they warrant. Shield tie length is extremely important in the effectiveness and quality of shielding. A shield tie that is short, less than 2 or 3 inches, is highly desirable; longer lengths, 6 inches or more, degrade the entire shield. The best termination is to the connector backshell. Future connectors will have backshells and filter pins that will need maintenance.

- Maintain electrical bonding and grounding quality. Careful surface preparation, proper joining techniques, care of bonding straps, and finally adequate conductive sealing of joints and seams ensure the continuation of the excellent shielding and electrical grounding provided by structure.

- Be aware of electrostatic discharge. Electrostatic discharge is a key intruder in handling and maintenance procedures. Microcircuits may be impaired or destroyed by a pulse from a hand or an item of clothing. The event can go unnoticed. Conductive materials and grounding procedures, along with a training program, will provide techniques for failure prevention.

### 3.4.4. Shielding and Shield Ties

Shields may be single braid; double braid; braid and foil; shields inside an overall bundle shield; solid conduit, tray, or cableway; and aircraft structure.

The shielding effectiveness (SE) of shields is based on materials, dimensions, circuit connections, impedances, and shield tie lengths and has been one of the most elusive electromagnetic compatibility protective defenses to pin down. (A significant issue for future aircraft needing to be addressed is that of the wiring lengths installed during laboratory tests versus the actual aircraft installed length.) Length influences SE and SE can dictate length or design. A single braided shield with a 2-inch shield tie may offer less than 25 dB of protection over the span of 10 kHz to 100 MHz. A long wire, 100 ft (30m), may only show 10 dB above 1 MHz at some resonant frequencies under certain conditions. A solid 360-deg connection to a backshell can improve protection. Conditions that establish the grounding of shields vary, but there are some that need emphasis:

- Ground audio or analog shields at receiver end only.

- Ground digital or wideband signal circuit shields at both ends.

- Ground shields subjected to high frequencies (greater than 50 kHz) at both ends.

- Ground shields that contain or are a barrier to transients at both ends.

- When audio and HF requirements conflict then the circuits and installation must be evaluated. (Solution may be rerouting of wires or double shielding.)

Carrying a shield tie through an avionics unit connector, into the internal wiring harness, and to a circuit card connector is poor wiring practice. A 360-deg, peripheral shield connection to the backshell is the best (figure 3.4-6).

## 3.5. Aircraft Protection Measures

### 3.5.1. Structure Conductivity

Conductivity is the predominant electromagnetic compatibility consideration of materials in the basic steps to a unified aircraft structure design (figure 3.5-1). What are the separate electrical functions so highly dependant on conductivity (figure 3.5-2).

- Electrical stability: A low noise ground reference plane - a stable zero reference foundation for electrical and electronic circuit and shield ties (may have less than 500-mV ground noise). This electrical "ground" embodies structure, shelving, skin, spars, equipment chassis, and possibly uniquely installed grids, sheets, and foil.

- Shielding: Aircraft structure, skin panels - foils, flame spray, plating, paint-shelves, equipment enclosures, and wire shields. Shielding affords a barrier to external and internal radio frequencies, 400-Hz electric fields, and 600V transients.

- Fault path: Structure, skin panels, cable shields, safety wiring (green wire). The engineered fault paths divert currents to assure safety of passengers and personnel, prevent hazardous voltages, avoid ignition of combustibles (fire prevention), and limit equipment failure and upset.

- "Diverter": Structure, skin panels. The aluminum aircraft inherently offers the current control paths and bypass to eliminate shock hazard and damage from electrostatic charge and lightning.

- Signal return and power return: Cost and weight savings accrue through the use of structure as a return instead of the installation of wire.

- Reliability and redundancy: Parts of the aircraft may be employed as a baffle or wall to provide separation of wiring or equipment.

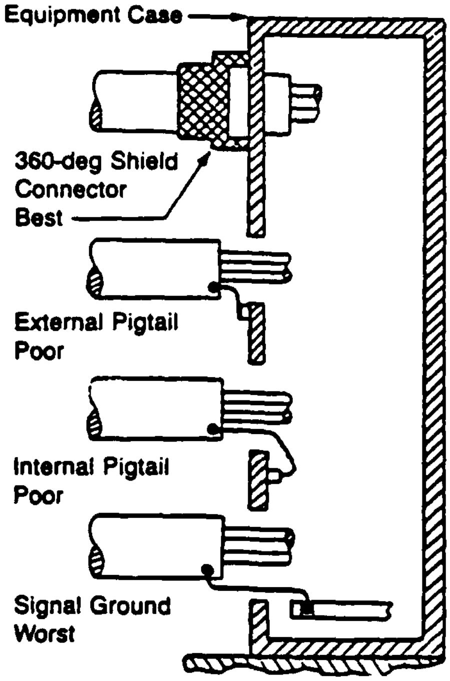


FIGURE 3.4-6. SHIELD TIES

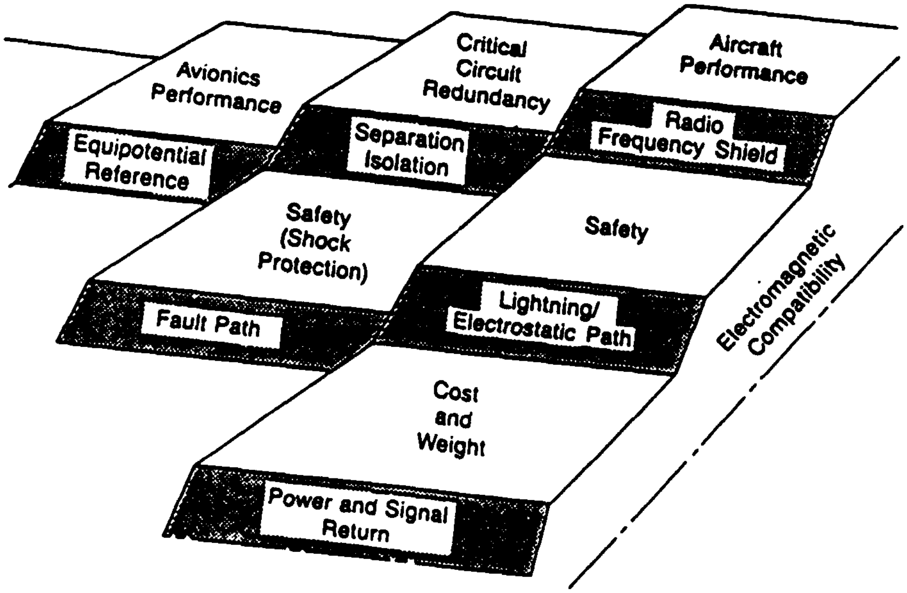
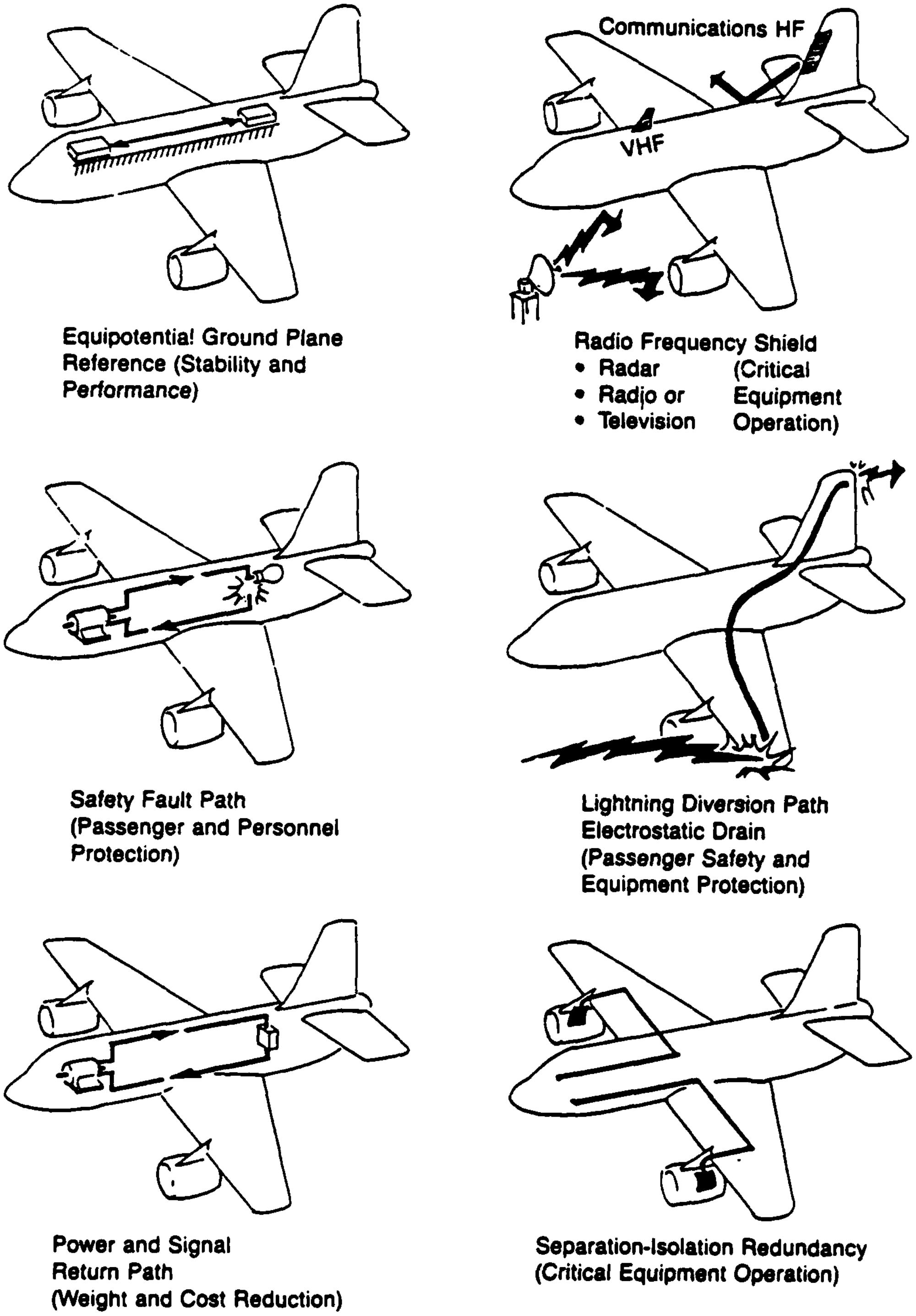


FIGURE 3.5-1. THE GROUNDING STEPS



Equipotentia! Ground Plane Reference (Stability and Performance)

Radio Frequency Shield
- Radar (Critical
- Radjo or Equipment
- Television Operation)

Safety Fault Path (Passenger and Personnel Protection)

Lightning Diversion Path Electrostatic Drain (Passenger Safety and Equipment Protection)

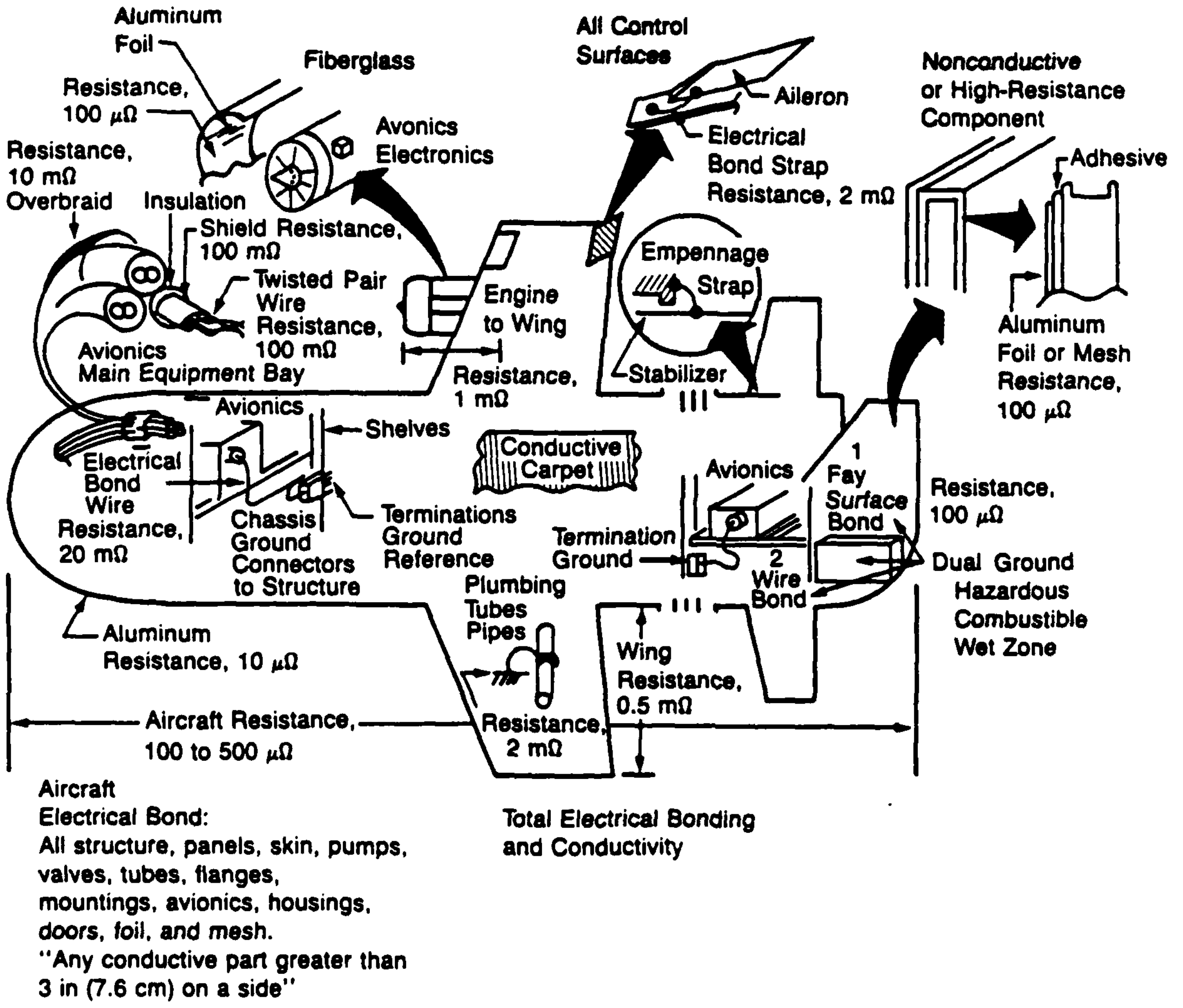
Power and Signal Return Path (Weight and Cost Reduction)

Separation-Isolation Redundancy (Critical Equipment Operation)

FIGURE 3.5-2. STRUCTURE EMC ROLES

The engineering of the structure, etc., to accommodate all of the electrical functions, entails detail design of electrical interfaces, bonding straps, foils, paints, etc. (figure 3.5-3). Bonding resistance tests can be made during the aircraft EMC test (see section 7).

It is illustrative and instructive to compare an aircraft with an electronics facility to help recognize the significance of the aluminum structure as a substantive electrical component (figure 3.5-4). Except for framing, many of the facility building materials are not conductive.



Aluminum Foil
Fiberglass
Resistance, 100 μΩ
Resistance, 10 mΩ
Overbraid
Insulation
Avonics Electronics
All Control Surfaces
Aileron
Electrical Bond Strap Resistance, 2 mΩ
Noncanductive or High-Resistance Component
Adhesive
Shield Resistance, 100 mΩ
Twisted Pair Wire Resistance, 100 mΩ
Avionics Main Equipment Bay
Engine to Wing
Resistance, 1 mΩ
Empennage
Strap
Stabilizer
Aluminum Foil or Mesh Resistance, 100 μΩ
Avionics
Shelves
Conductive Carpet
Electrical Bond Wire Resistance, 20 mΩ
Chassis Ground Connectors to Structure
Terminations Ground Reference
Avionics
1 Fay Surface Bond
Resistance, 100 μΩ
Termination Ground
2 Wire Bond
Dual Ground Hazardous Combustible Wet Zone
Plumbing Tubes Pipes
Aluminum Resistance, 10 μΩ
Wing Resistance, 0.5 mΩ
Aircraft Resistance, 100 to 500 μΩ
Resistance, 2 mΩ
Aircraft Electrical Bond:
All structure, panels, skin, pumps, valves, tubes, flanges, mountings, avionics, housings, doors, foil, and mesh.
"Any conductive part greater than 3 in (7.6 cm) on a side"
Total Electrical Bonding and Conductivity

FIGURE 3.5-3. DETAILS AND INSTALLATION

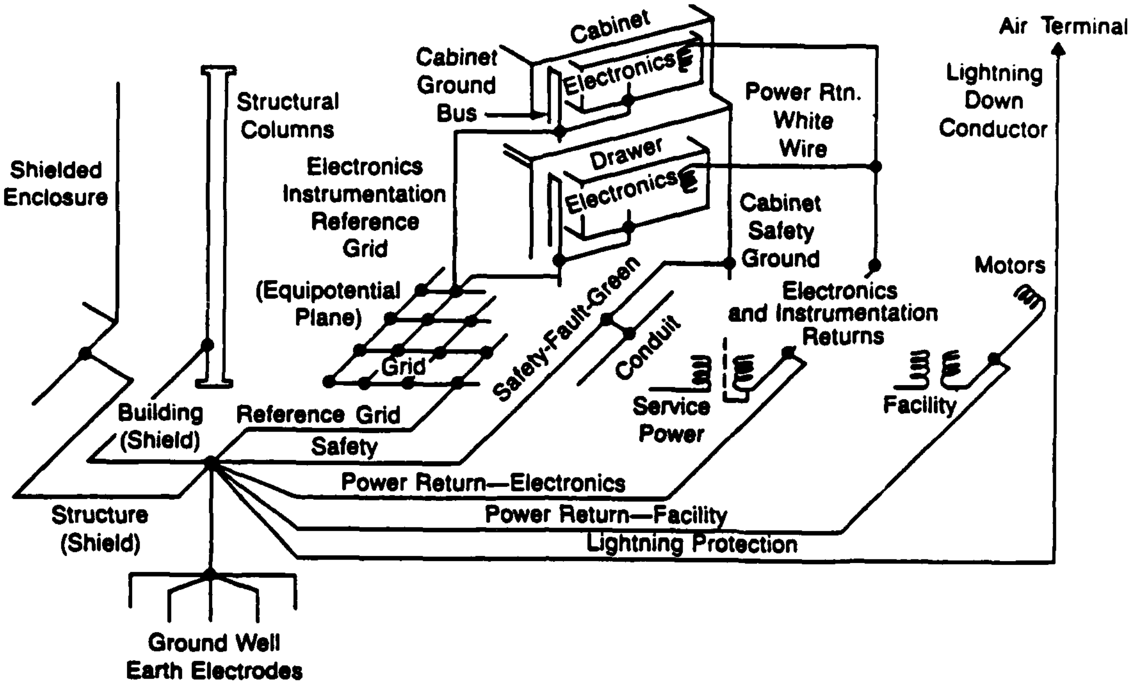


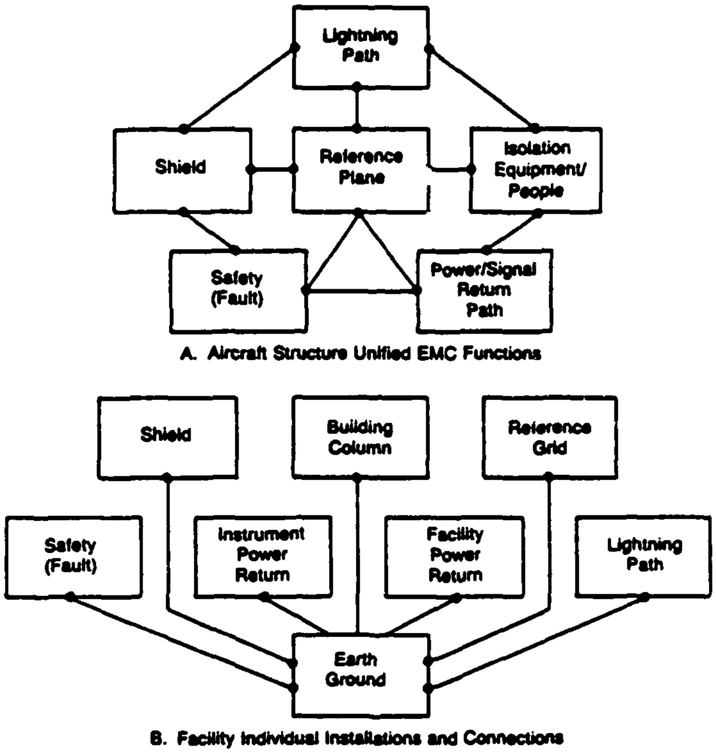
FIGURE 3.5-4. THE SEVEN EARTH GROUND CONNECTIONS

The electrical functions so freely supplied by the airplane structure must be built into a properly constructed facility using extra materials and supports. Whereas the airplane unifies the functions, in the facility they are separate (figure 3.5-5).

## 3.5.2. Shielding

Aluminum, after copper, is one of the best electromagnetic shields. Its effectiveness varies with thickness and frequency. One or two thousandths (1 or 2 mils) is good (figure 3.5-6).

Wherever shielding, grounding, or conductive properties are lost at joints and seams (figure 3.5-7) or are not available from structure (therefore compromising continuity), shielding must be added. Aluminum foil, flame spray, plating, and paint are candidate solutions (figure 3.5-8).



A. Aircraft Structure Unified EMC Functions

B. Facility Individual Installations and Connections

FIGURE 3.5-5. EMC ANATOMY BLOCK DIAGRAM

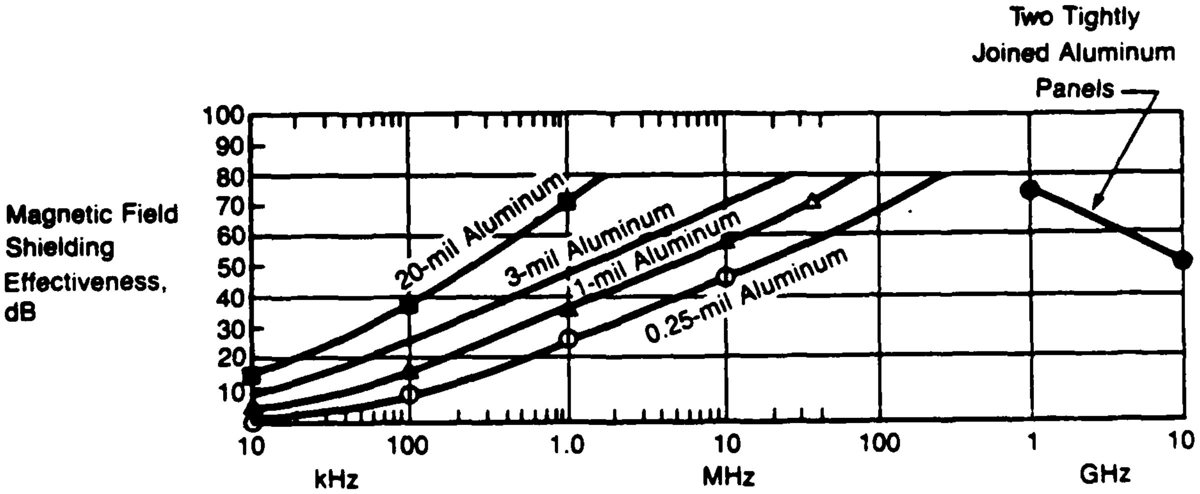


FIGURE 3.5-6. MAGNETIC FIELD SE OF ALUMINUM

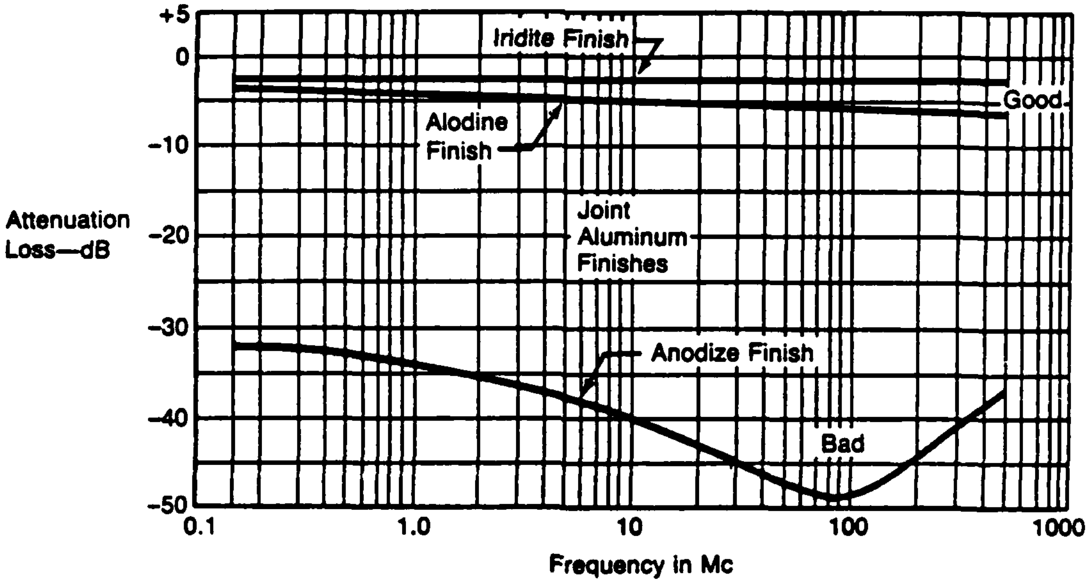


FIGURE 3.5-7. LOSS OF SE WITH JOINT FINISH

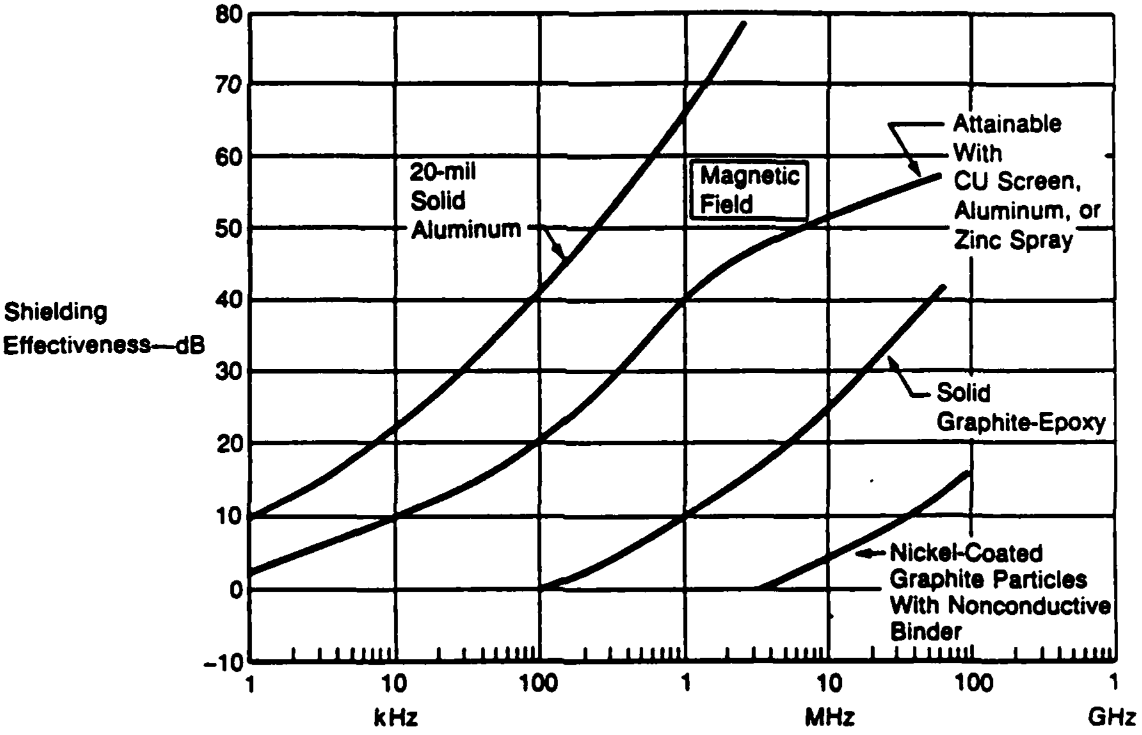


FIGURE 3.5-8. SE COMPARISON

Foil (aluminum or copper) is a good shield, conductor, and reference plane. Foil may bring with it an increased effort to establish quality of bonding to adjacent parts, reliability under environment and vibration, and integrity and durability. Moreover, the foil size, thickness, and geometric configuration dictate its economy of installation. Foil can make a good wire shield.

Flame spray applications (aluminum, copper, or zinc), even by skilled operators, can be difficult to apply in a controlled fashion. The resistance of flame spray coatings is higher and shielding effects lower even with greater thicknesses than foil. Its dense coat and coarse finish on a substrate can lead to flaking or cracking under vibration and moisture conditions with obvious loss of qualities.

Paints (metal or containing conductive agents or fillers) provide good shielding and are used successfully. Insulating or moderately resistive material (graphite-epoxy) may be painted to provide shielding or conductivity or they may be overlaid with aluminum mesh or foil.

Wire shielding provides another layer of protection (figure 3.5-9). Aircraft structural shielding is an important companion to wire shielding. The levels of shielding effectiveness are computed for each wiring run location and configuration to determine the accurate values and these can then be combined with modeled and calculated values of structural shielding. Figure 3.5-10 shows some SE levels for silver or gold film that might be deposited on glass and aluminum or copper screen that could be for shielding ventilation ports on equipment. The front and rear spar areas exhibit very poor shielding. The figures depict nominal or typical estimated levels. Shielding exhibits such wide spreads and variations around these levels (dependant on conditions), and especially as frequency varies that these summary representations are useful as a tutorial tool, but are not appropriate as a design tool.

### 3.5.3. Safety in Grounding and Returns

Structure is a ground and a return. Seven separate grounds or returns on electrical/electronic equipment can be identified. Some of these ground/returns are interconnected and perform common functions. Certain individual grounds are always separated to avert mixing noisy and sensitive circuits.

- Case enclosures or housings (electrical/electronic equipment) ground: May be a wire or the case surface. This case enclosure ground acts as a safety ground (fault return), a static ground, and a radio frequency ground. It sometimes is a signal return and possibly a 115V, 400-Hz return.

- 115V, 400-Hz return: Isolated and brought out of the equipment on a separate wire (figure 3.5-11). A twisted pair power supply circuit will improve electromagnetic compatibility.

- 28V, 400-Hz return.

- 28V, dc return.

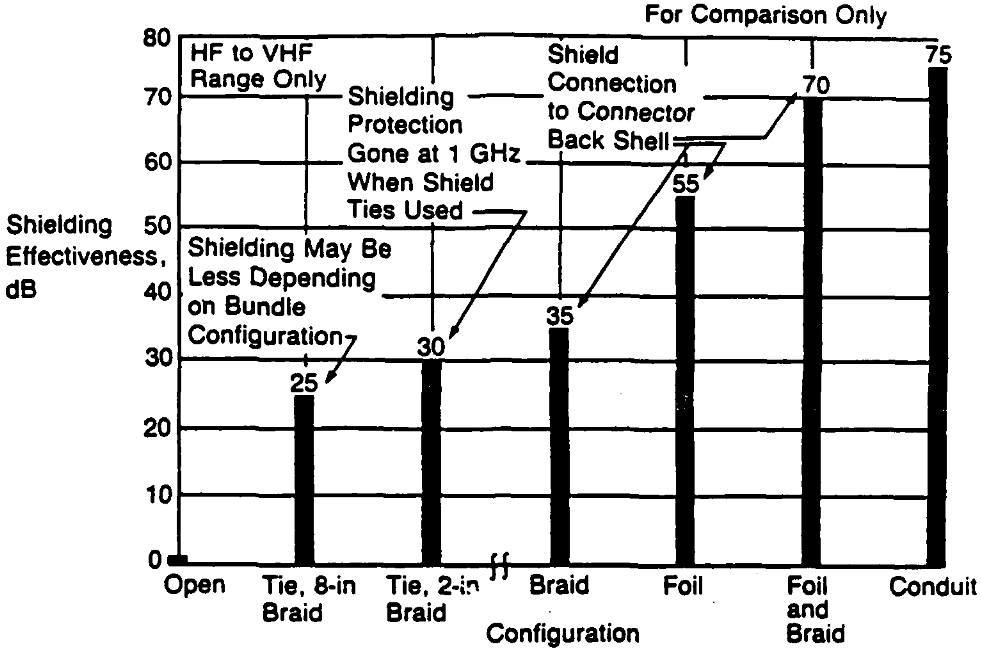


FIGURE 3.5-9. WIRE SE COMPARISON AT HF-VHF

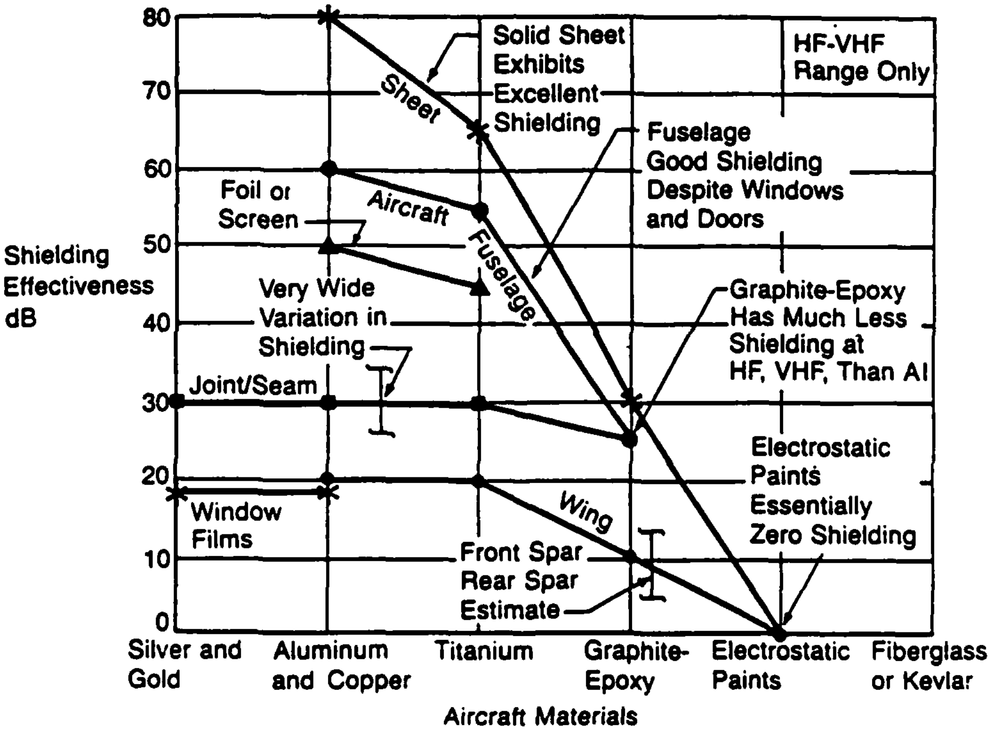


FIGURE 3.5-10. MATERIAL/CONFIGURATION SE OVERVIEW

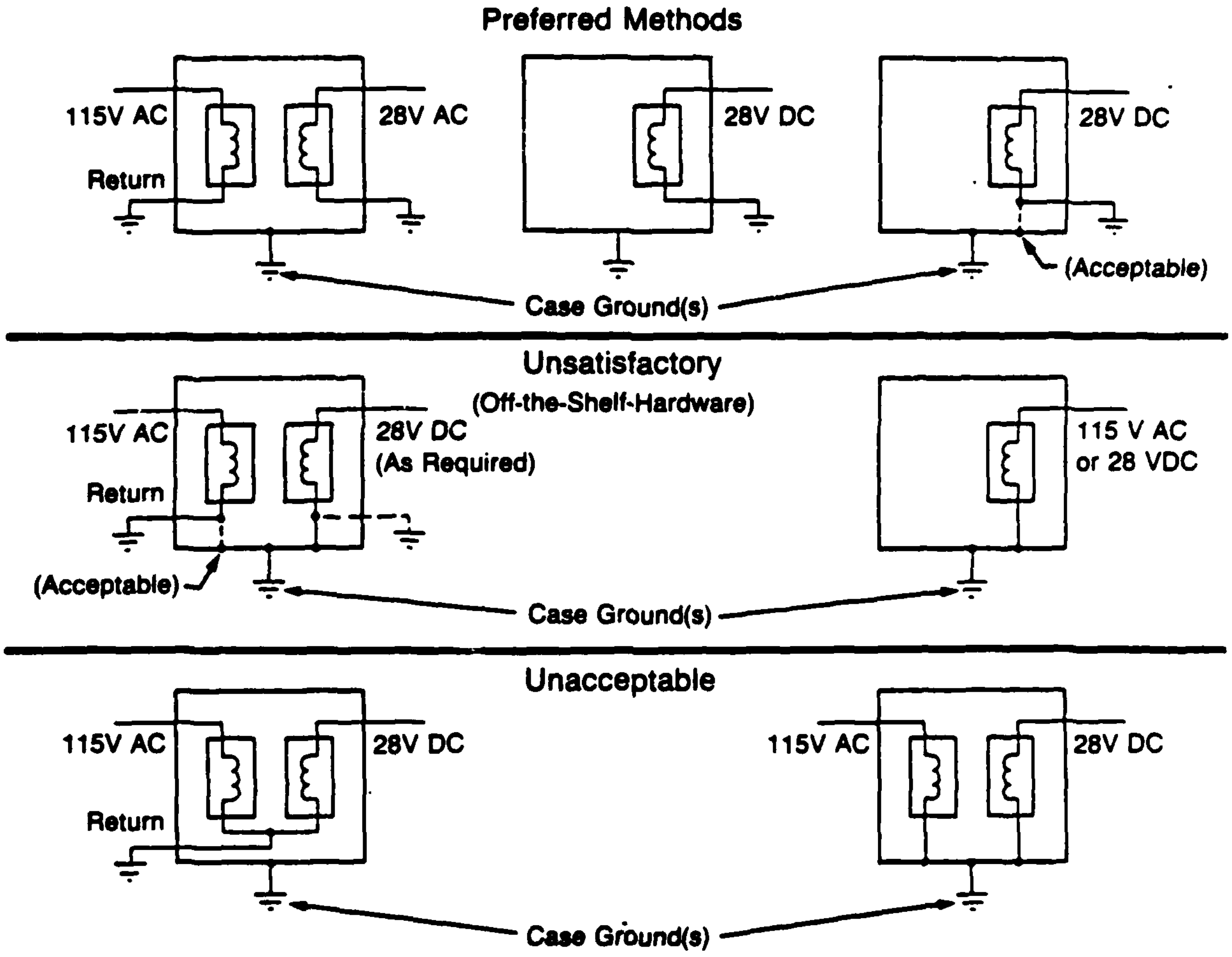


FIGURE 3.5-11. POWER RETURNS

- Audio or analog circuit return.

- Digital circuit return.

- Shield ties (pigtails).

Certain case enclosures require dual grounding in a flammable leakage zone or water exposure area, possibly around wing, cargo, and tail locations, to offer redundancy and safety in case of electrical fault. Power returns are brought out of these zones before being terminated to structure. Each circuit is exhaustively reviewed for voltage, current, resistance, and potential voltage drop at each connection. MIL-B-5087 gives resistance limits of 6 mΩ to 11 μΩ maximum when computed fault currents are 50A to 7 kA.

3.5.4. Resistance

Two and one-half milliohms (0.0025Ω) is the most often quoted resistance maximum for a termination or connection when designing for electromagnetic compatibility. It is applied to wire terminations, case enclosures, mounts, shelves, panels, doors, and radio frequency components. The 2.5-mΩ limit is appropriate wherever any component or structure forms a part of the ground plane, shielding, fault path, or power or signal return.

Panels, rails, frames, access doors, and all conductive items in the flight deck are bonded especially to reduce electrostatic discharge.

Pumps, valves, flanges, lines, vents, and penetrations in the fuel tank are bonded especially to prevent arcing from lightning. Transport aircraft undergo thorough research and assessment of conductivity or resistance. It is sometimes difficult to attain 2.5 mΩ. The resistance of aluminum is a good basis for comparison of other materials (figure 3.5-12 and figure 3.5-13).

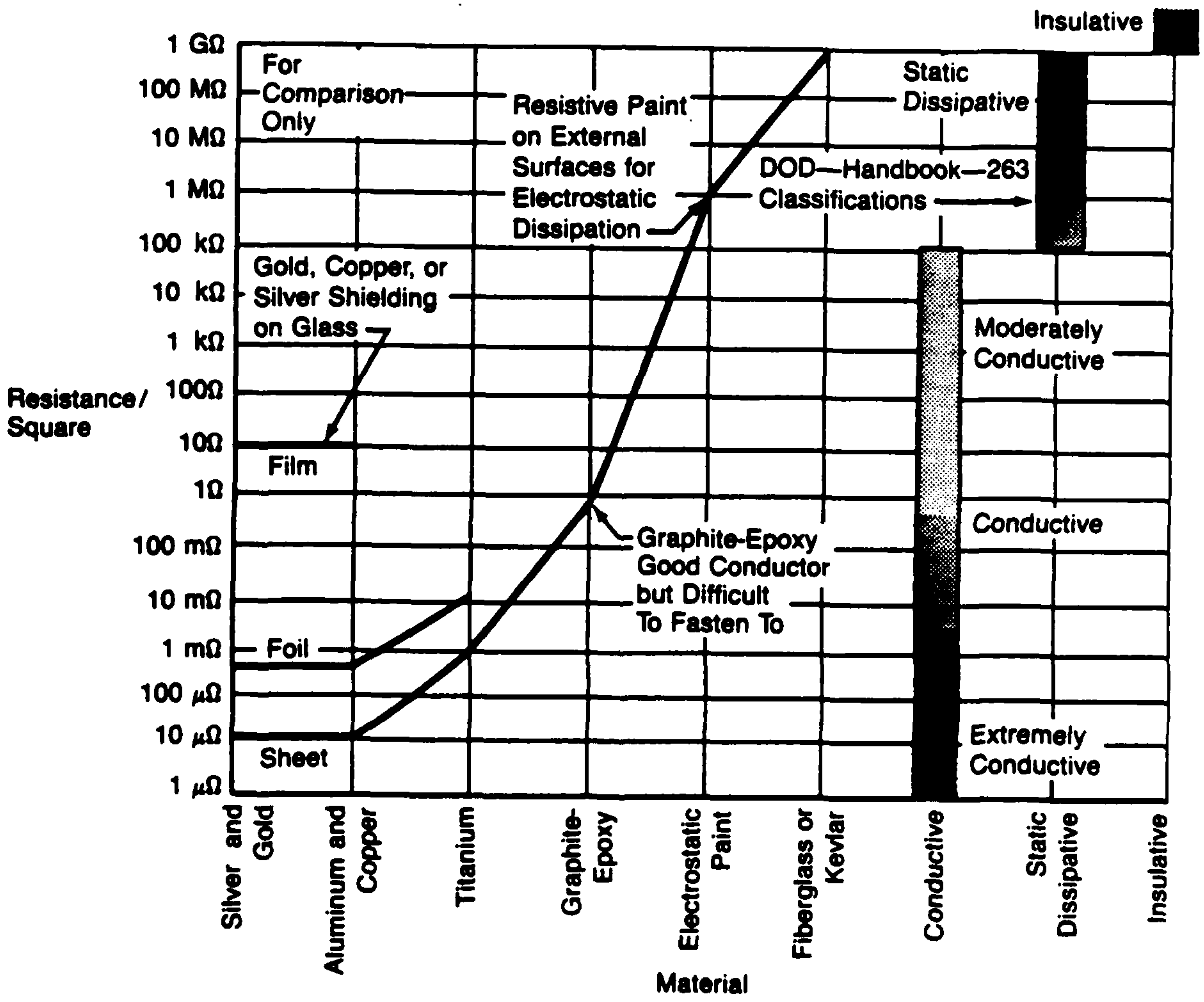


FIGURE 3.5-12. MATERIAL/RESISTANCE OVERV:EW

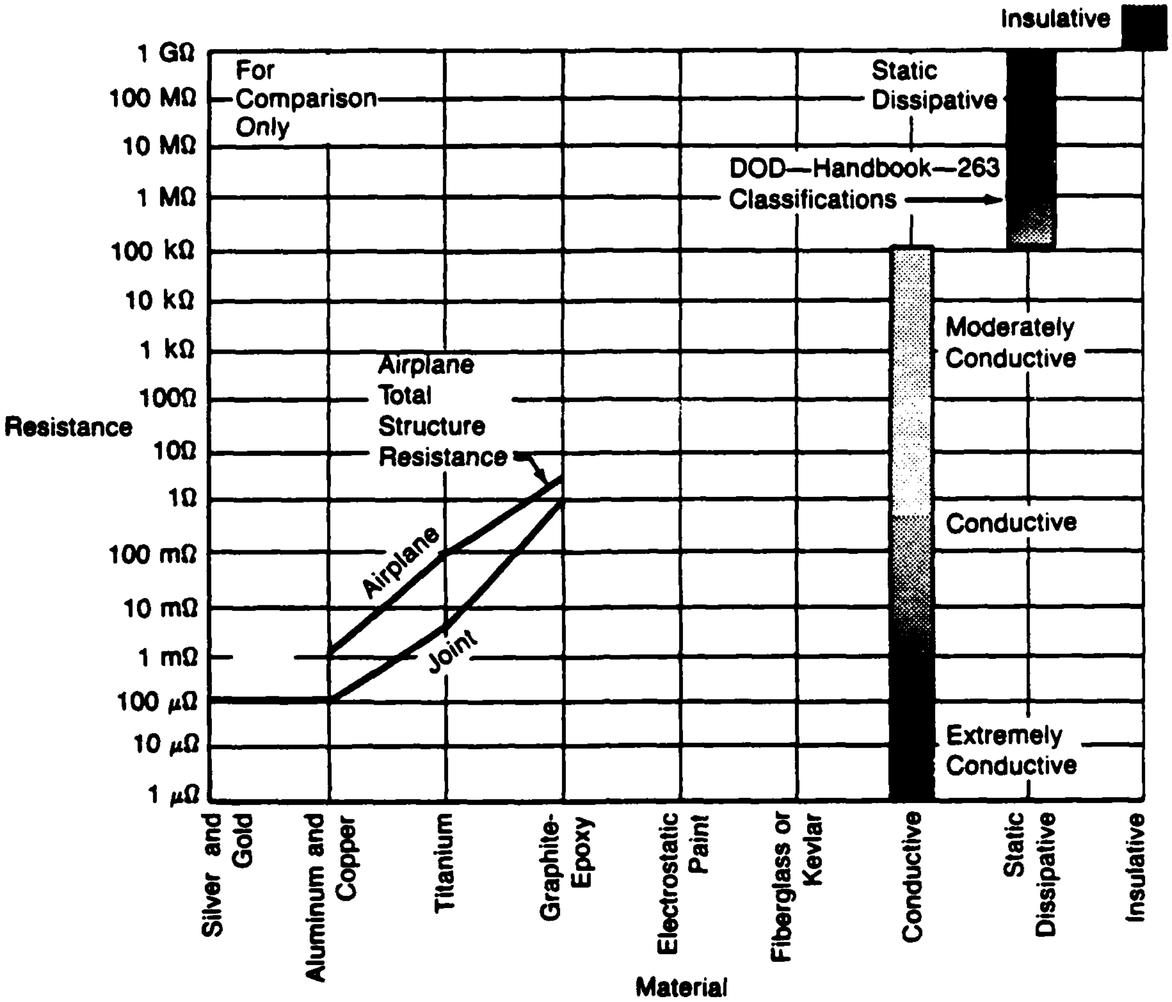


FIGURE 3.5-13. CONFIGURATION/RESISTANCE OVERVIEW

Ground planes establish the electrical foundation for any system. Copper is practical, affordable, and is usually employed in the electromagnetic compatibility laboratory (figure 3.5-14). Currents flowing in copper have a low IR drop and therefore provide a low noise system. Aluminum usually offers good conductivity through faying surface bonds or permanent joints. A number of factors affect resistance: pressure and surface finish are significant (figures 3.5-15 and 3.5-16).

When components do not form a part of the electrical design but must be grounded for safety, a 1Ω resistance is often adequate. Where electrostatic charge buildup is of concern on nonconductive materials such as on external dielectric surfaces, the resistance limit may be allowed to be much higher. Military Handbook 263 gives 500 kΩ to 100 MΩ as the range to adequately drain away electrostatic charge.

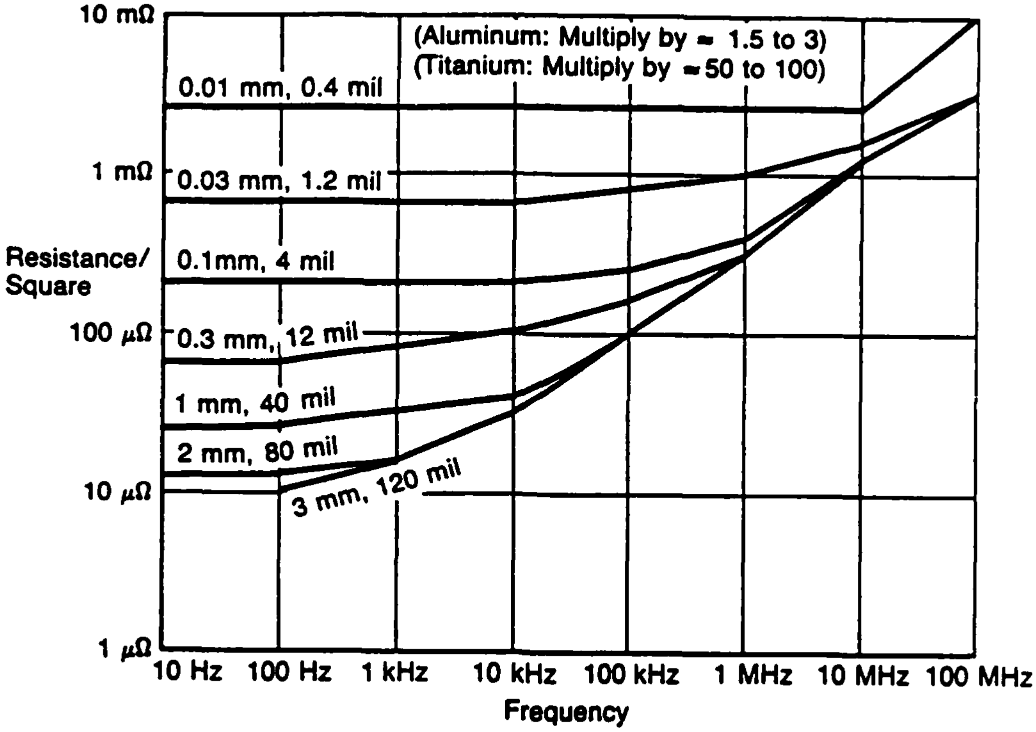
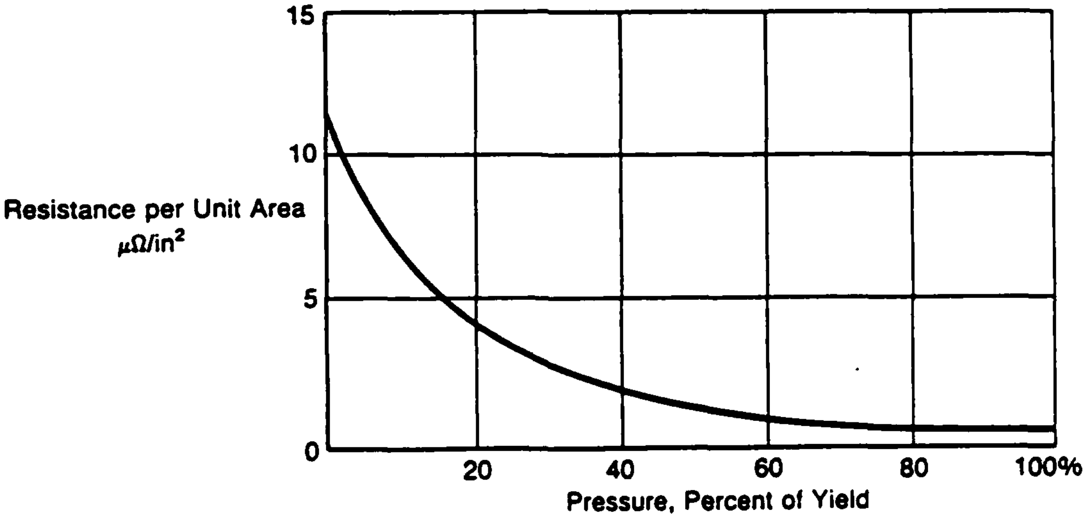


FIGURE 3.5-14. RESISTANCE PLOT - COPPER PLANE



Sections of 2024 Aluminum Alloy Under Compression With Joint Sanded Prior to Test

FIGURE 3.5-15. RESISTANCE VERSUS PRESSURE

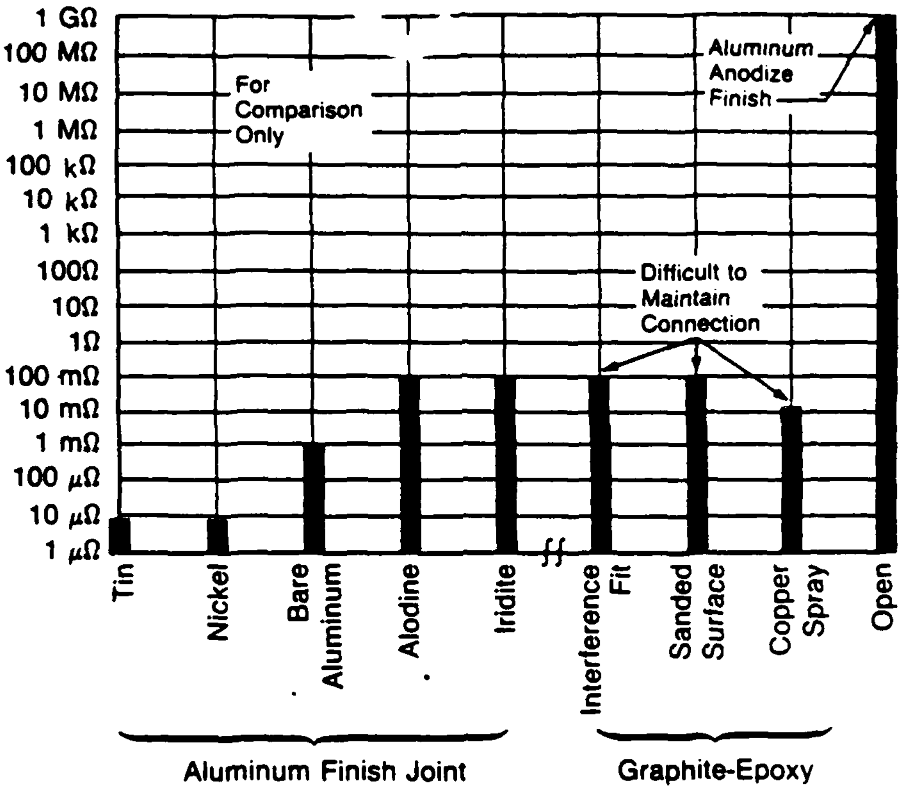


FIGURE 3.5-16. JOINT FINISH RESISTANCE

In summary, the complexity of the joining process and its maintenance is contrasted by the simplicity of the electrical bonding resistance limit: 2.5 mΩ. Aluminum is the grand conductive foundation. The part that it plays cannot be overstated. It stabilizes, shields, conducts, isolates, and protects.

### 3.5.5. Resonance

Aluminum structure and single wires as conductors have a drawback. They resonate (figure 3.5-17). Structure and single wires must be avoided in high-frequency circuit design.

## 3.6. Composites

Graphite-epoxy is a fair to good conductor and shield.

Kevlar and fiberglass are insulators and have no affect on radio frequency fields. Dielectric structural materials need to be modified to provide electromagnetic shielding.

Nonmetallic materials form many parts in today's aircraft (figure 3.6-1) and are expected to increase in the future. When varieties of materials are brought

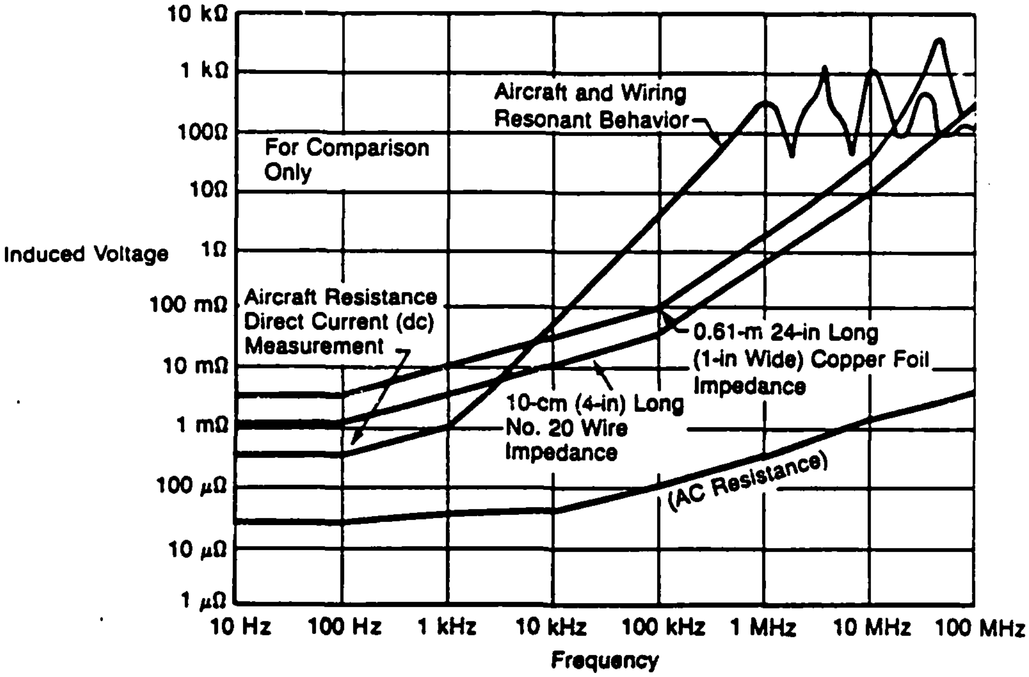


FIGURE 3.5-17. AIRCRAFT AND STRAP RESONANCE

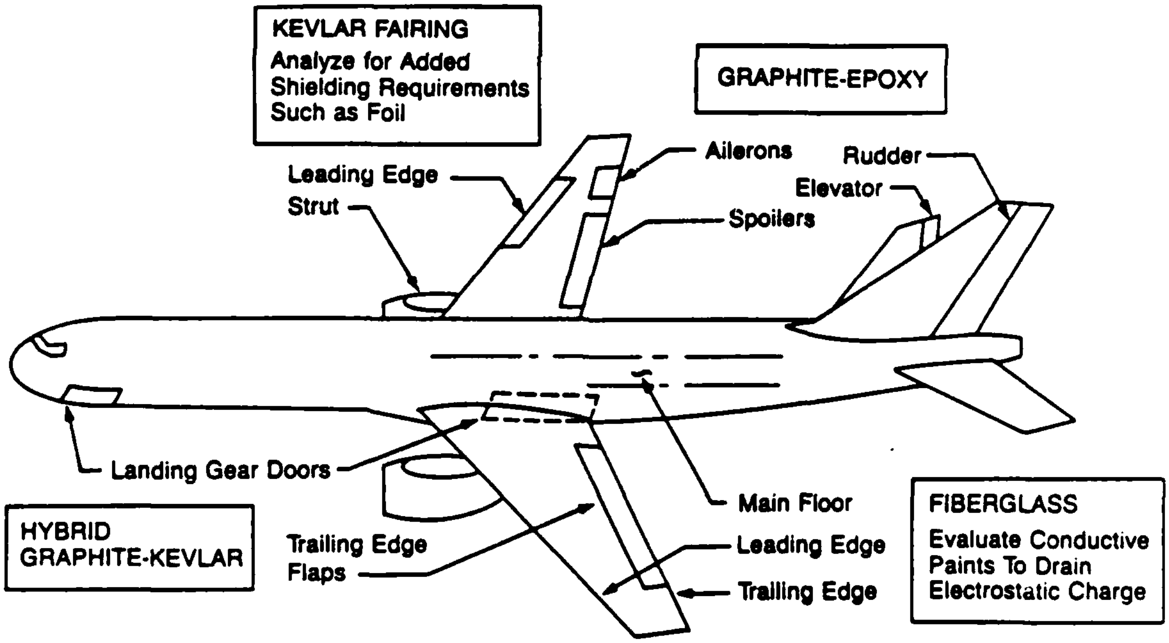


FIGURE 3.6-1. TYPICAL NONMETALLIC APPLICATIONS

together, the interfaces lead to escalating possibilities of material mismatch between finishes, fasteners, and adhesives with possible adverse implications for the quality of electromagnetic compatibility.

Graphite-epoxy will conduct and will shield. Electric field shielding is very good. Following is a comparison of appropriate electromagnetic compatibility-related characteristics:

- Dc resistivity: more than 1000 times greater than aluminum in longitudinal direction and 100 thousand to 1 million in the transverse direction.

- Joint resistance: 30 mΩ to 1Ω or higher. It is difficult to create an electrical connection to graphite-epoxy, and once the connection is made, it is difficult to maintain. New techniques and better procedures are being developed. Today, graphite-epoxy cannot be used as a power or signal return.

- Magnetic shielding starts at about 1 MHz, rises to 60 dB at 100 MHz with about 35 dB in the HF-VHF range.

If graphite-epoxy is not well bonded at seams and joints, it will not act as a shield.

If composites are used extensively for structure, the greatest impact is in providing for a ground plane, the signal return system, and the power return system, which will require their own installations of wire, conductive foils, strip, or cableways. Graphite-epoxy resistance is too high to provide an adequate ground plane (except for antennas). Figure 3.6-2 shows the general level of resistance of a large cylinder or tube, and indicates that its use as a power return path and signal return path is unsatisfactory.

If graphite-epoxy or insulating materials are built into the structure, loss of shielding may open up a path for noise from fluorescent lights, switching regulator and clock oscillator harmonics to reach the ADF, HF, or VHF receivers. Or, in turn, HF frequencies may enter wiring and the avionics. The effects of radio frequency electromagnetic interference are becoming more of a concern (figure 3.6-3). Figure 3.6-4 illustrates some of the resistance levels that might be encountered and shows the use of twisted pair or twisted pair shielded wire.

In the world of electromagnetic compatibility, our protection and safety lies in an integrated design: architectural or structural shielding, shielded wiring, interface circuit voltage limiters, and software correction techniques. The soul of electromagnetic compatibility is a balanced, isolated, shielded interface circuit: it is practically impervious to conductive, inductive, and capacitive attack of electrical noise.

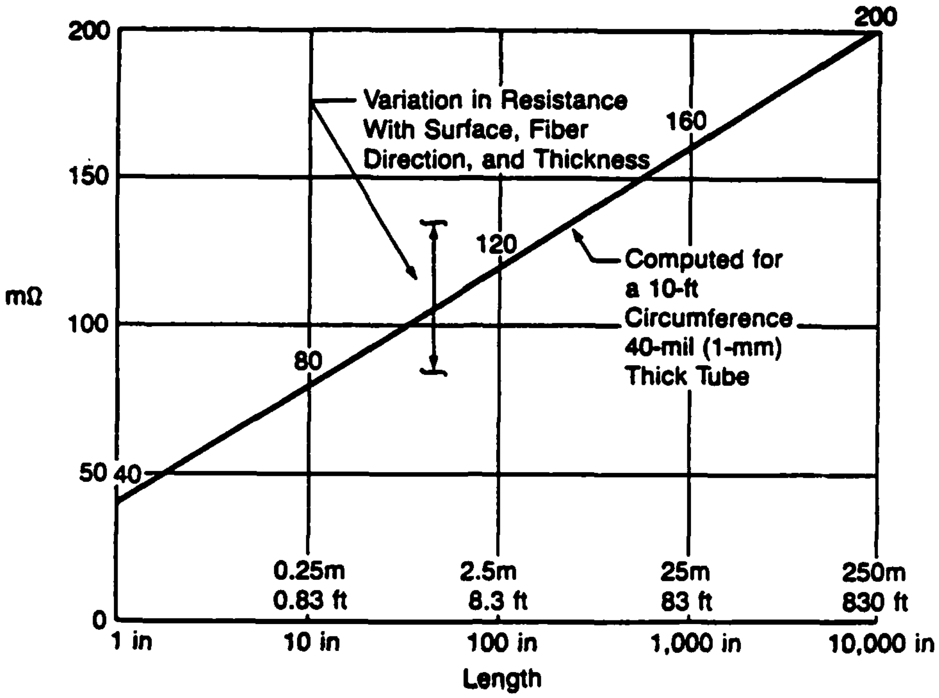


FIGURE 3.6-2. GRAPHITE-EPOXY RESISTANCE

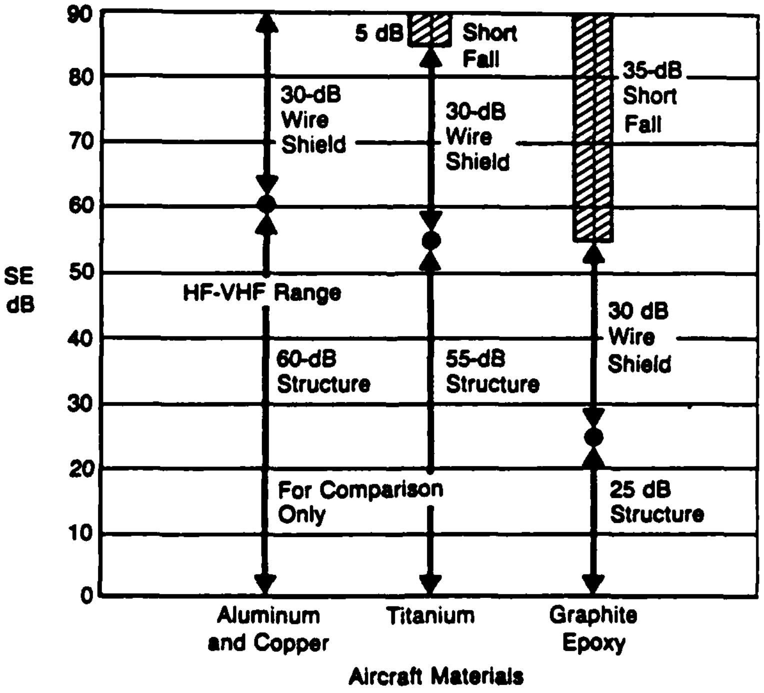


FIGURE 3.6-3. GRAPHITE-EPOXY SE SHORTFALL

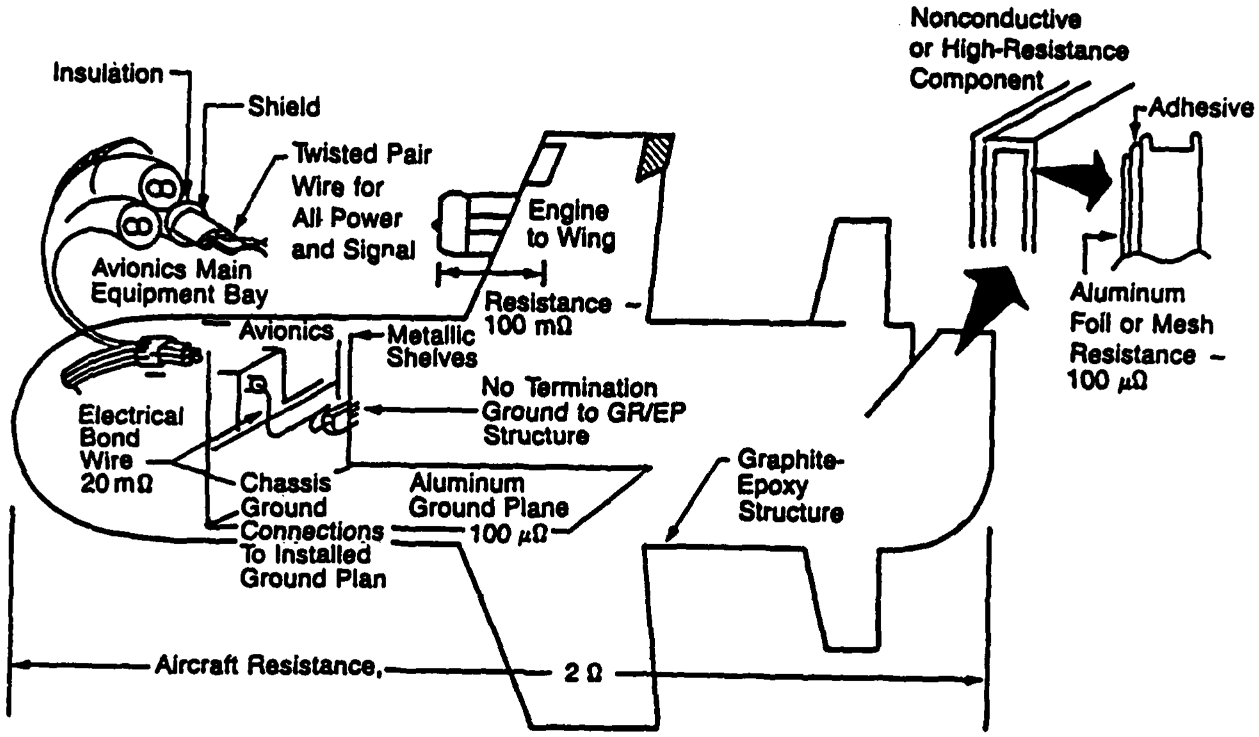

Insulation
Shield
Twisted Pair Wire for All Power and Signal
Avionics Main Equipment Bay
Engine to Wing
Resistance - 100 mΩ
Nonconductive or High-Resistance Component
Adhesive
Aluminum Foil or Mesh Resistance - 100 μΩ
Avionics
Metallic Shelves
No Termination Ground to GR/EP Structure
Electrical Bond Wire 20 mΩ
Chassis Ground Connections To Installed Ground Plan
Aluminum Ground Plane 100 μΩ
Graphite-Epoxy Structure
Aircraft Resistance, 2 Ω

FIGURE 3.6-4. GRAPHITE-EPOXY DETAILS AND INSTALLATION

# 4. EMC ANALYSIS AND ENVIRONMENT

## 4.1. Radiated Environment

### 4.1.1. Radio Frequency Field Distribution

#### 4.1.1.1. Environment

The electromagnetic radio frequency spectrum is vast. Electromagnetic radio frequency field strengths - measured in volts per meter - vary widely. But how do we bind them and treat them so we understand their significance? Well, for the purposes of electromagnetic interference simplicity, one might say we, as humans, and the aircraft, as an object, exist in a dimensional world of roughly 300m to 1m which, converted to radio waves, is 1 MHz, to 300 MHz.

That is very important for electromagnetic compatibility.

The American National Standards Institute (ANSI) radio frequency protection guide for personnel has the strongest field strength limitation over the span of 3 to 300 MHz. People, airplanes, wiring, and the avionics equipment itself are most susceptible to the frequency spectrum spanning the range of 1 to 300 MHz. This is the HF-VHF range (figure 4.1-1). The conditions and behavior of radio frequencies are sometimes so complex that radio frequency measurement and design efforts have often been given the title of "black art." Stray fields, cavities, diffraction, absorption, resonance, constructive interference, destructive interference: all of these interact to make the details of radio frequency studies conceptually difficult over some of the transitional frequency ranges.

The spectrum of radio frequency fields that penetrate aircraft wiring and enter into the avionic inputs to attack integrated circuits can be bounded and summarized over three basic regions:

- A low frequency below 1 MHz where radio frequency noise is normally less of a concern because fields are very inefficiently received on a wire.

- The HF and VHF region, 1 to 300 MHz, where radio frequency fields are very much of a concern and aircraft wiring acting as an antenna is efficient.

- An upper frequency range above 300 MHz where induced voltages in wiring drop off rapidly with increasing frequency and are easier to control.

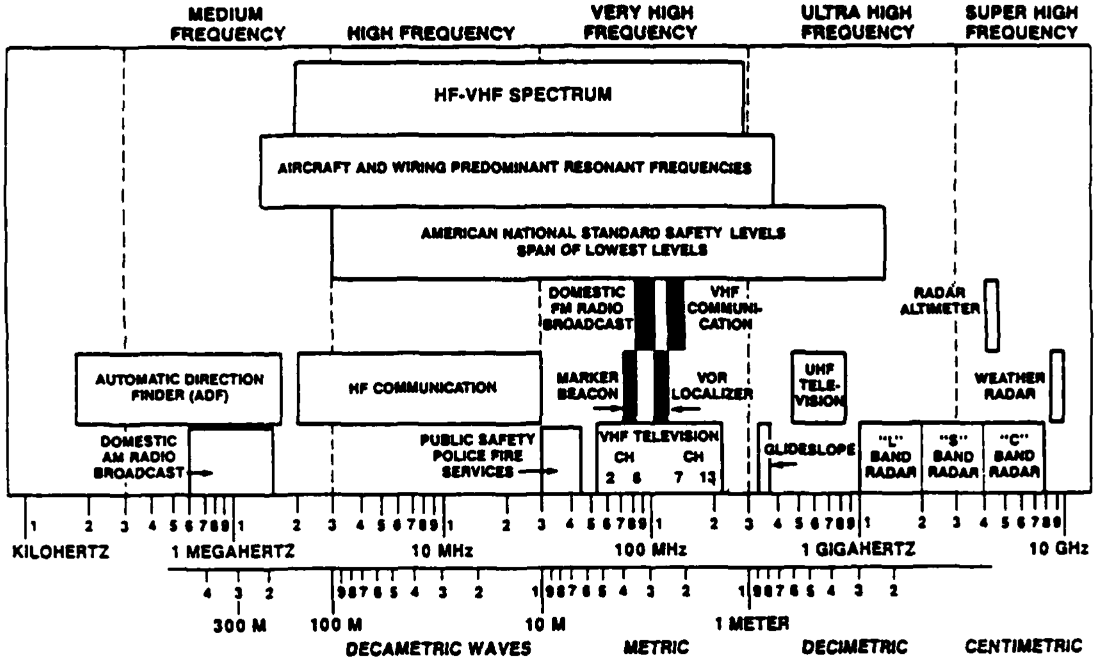


FIGURE 4.1-1. HF-VHF RANGE

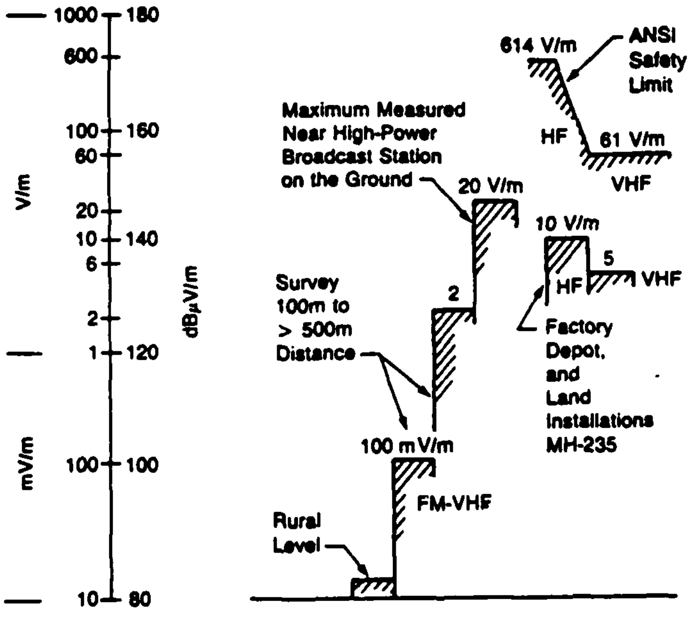


FIGURE 4.1-2. SELECTED RF FIELDS: HF-VHF RANGE

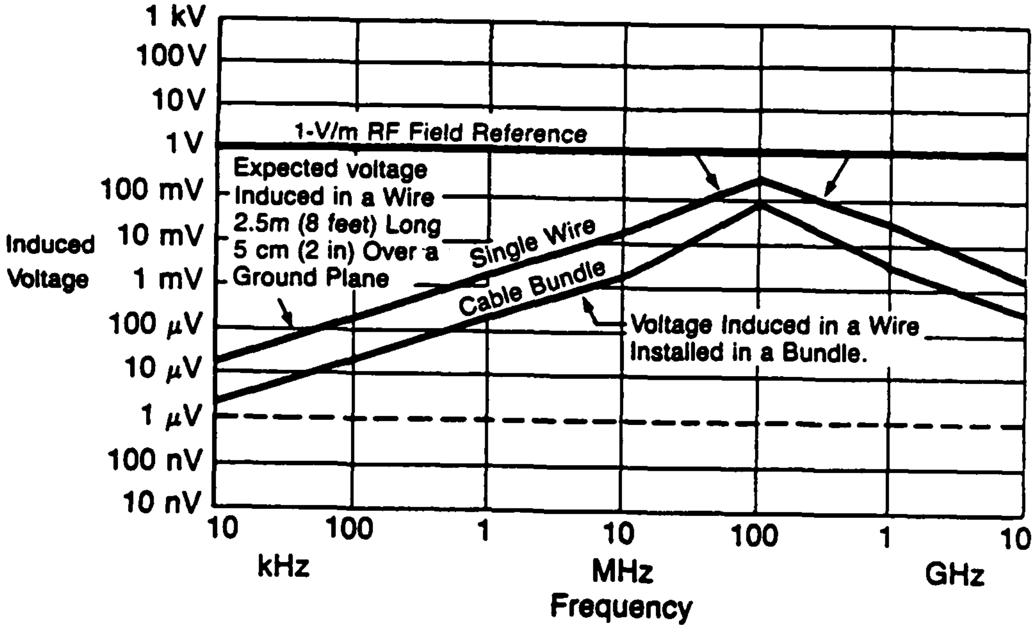


FIGURE 4.1-3. EXPECTED WIRE VOLTAGE - EIGHT FEET

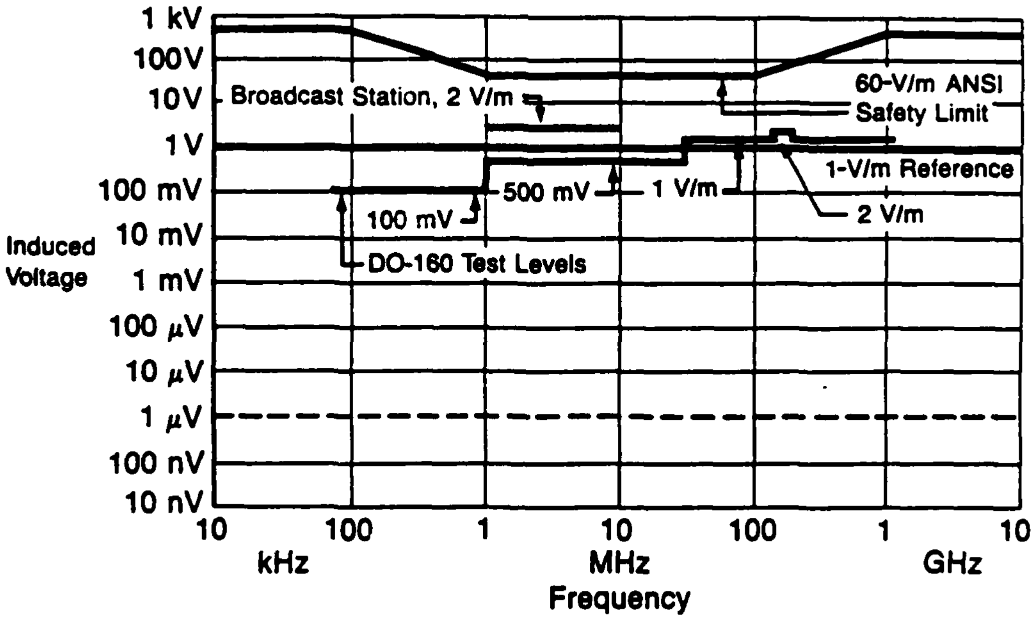


FIGURE 4.1-4. ENVIRONMENTS, SAFETY, AND TEST

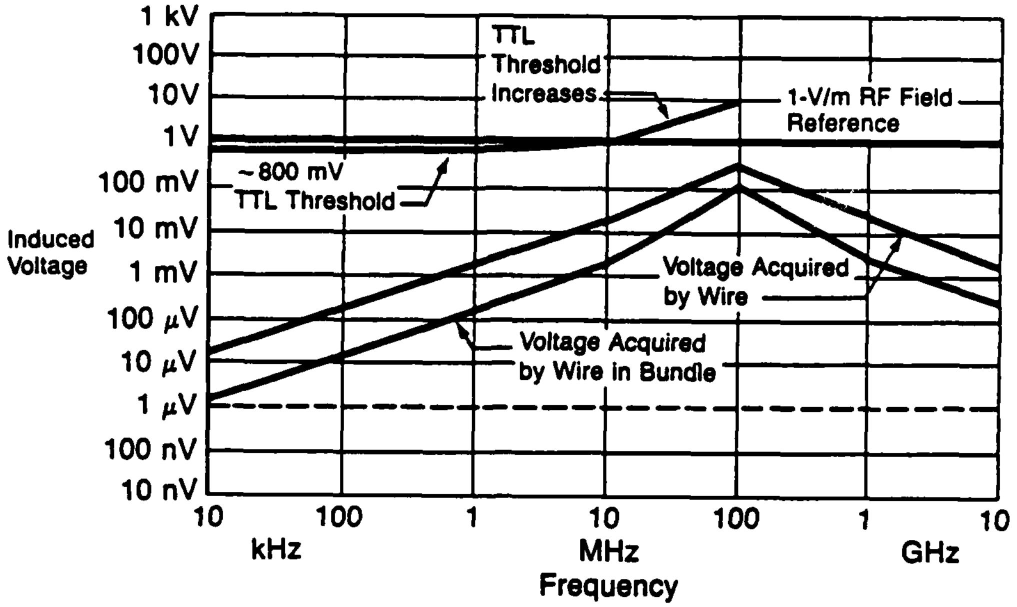


FIGURE 4.1-5. TRANSISTOR THRESHOLD

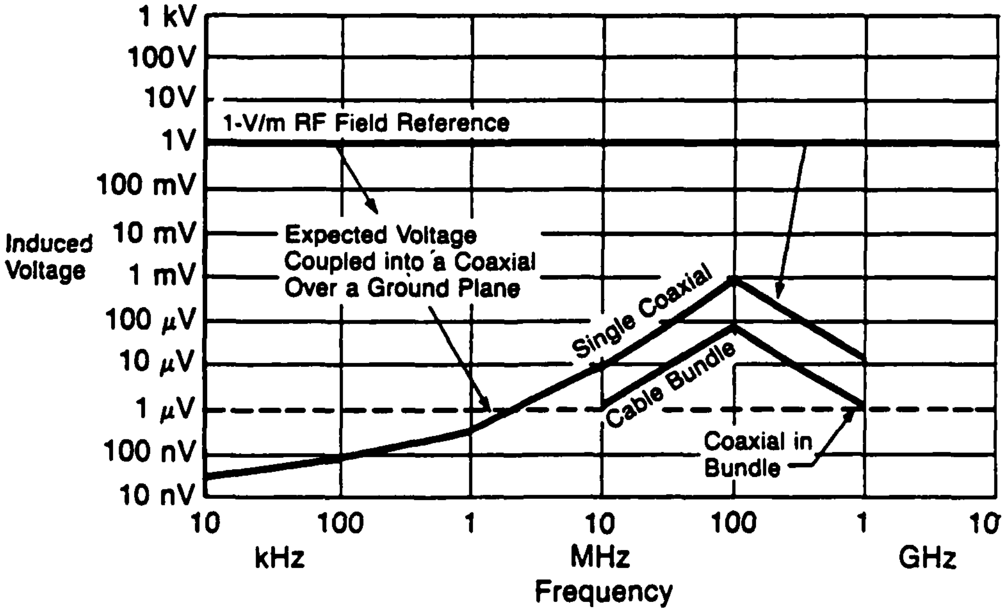


FIGURE 4.1-6. REPRESENTATIVE COAX VOLTAGE COUPLING

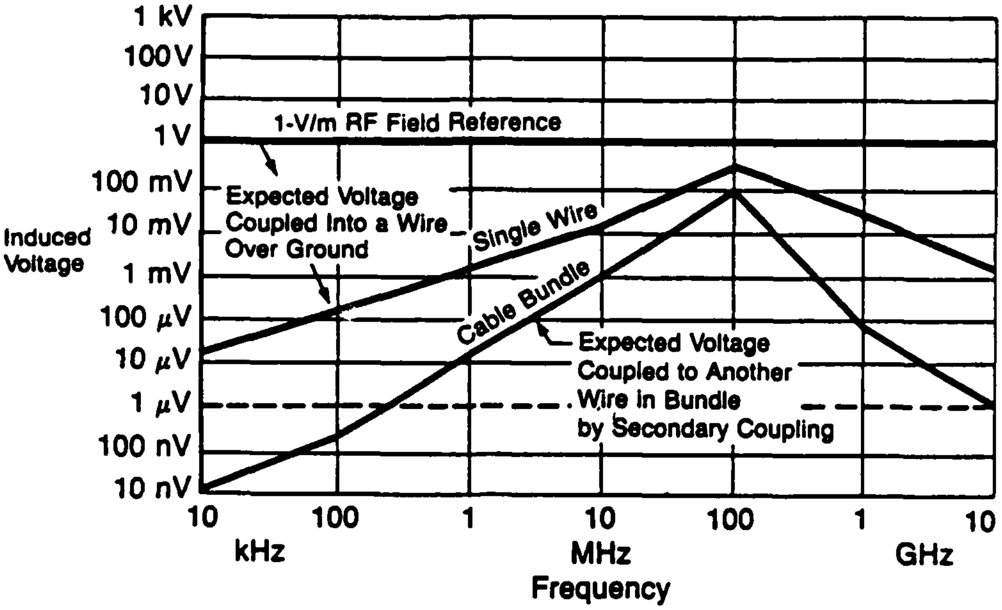


FIGURE 4.1-7. REPRESENTATIVE SECONDARY COUPLING

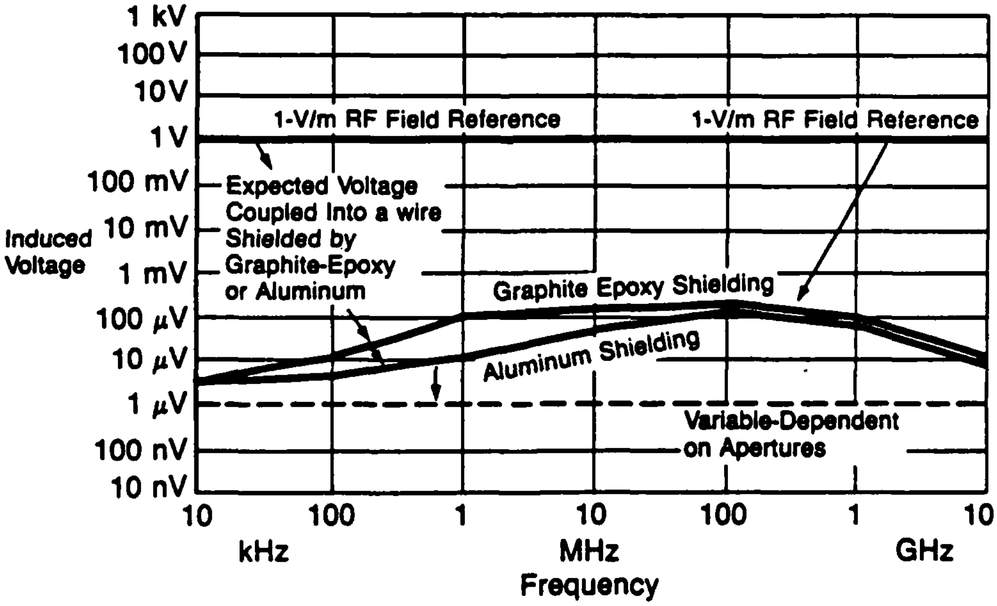


FIGURE 4.1-8. GRAPHITE-EPOXY OR AL SHIELDING ADDED

HF and VHF, ground-based FM radio and TV broadcast signals join with their airborne companions, the aircraft HF and VHF communication links, to induce significant voltages on aircraft wiring in the 1- to 300-MHz range. HF-VHF field strengths measured at ground level for selected urban, suburban, and rural areas are plotted in figure 4.1-2. At altitude, stronger fields can exist (see section 10, Bibliography, ECAC study). The ANSI personnel safety limit and the Military Handbook 235 Environmental Test Specification are plotted for comparison.

Figures 4.1-3 through 4.1-8 give a general view of the expected induced voltages (in some specific wires under selected conditions) and also a comparison of related environments. This information and data is illustrative and advisory to resolve significance and make comparisons of parametric properties and behavior and is not for use or adaptation to specific designs.

Aircraft structures and avionics are engineered and designed by the airframe manufacturer and subcontractors to limit and control these fields. Some lines are shielded, some filtered, and others incorporate a balanced circuit design that will very effectively reject most radio frequencies.

Another main defense against HF-VHF radio frequency signals is a comprehensive and all-inclusive electrical bonding system of all aircraft structural shielding materials to eliminate resistive seams and open seams or apertures. During a specific design program, it is becoming more and more necessary to develop a sophisticated set of models and computations to characterize and define the particular installation and uncover the behavior of the radio frequency fields and induced voltages.

So, in summary, the HF-VHF frequencies are important to aircraft designers because the wiring, equipment, structure, and the aircraft itself, having the same dimensions as the radio frequencies, become efficient antennas.

### 4.1.1.2. Resonant Behavior

Resonance is the ingredient that brings the arcane aspect to electromagnetic interference. Resonance, standing waves, and reflections share a commonality with black magic in their illusory and unseen character. Electrical parameters, voltage, and current, under the influence of the infinite variability of resistance, capacitance, and inductance, depending on the number of electrical poles, and when viewed over the frequency spectrum, may start out with high impedance and fall quickly to a short circuit minimum. Then they curve back to a maximum. On the other hand, the impedance may start low and rise to open circuit values. Voltage and current in RLC circuits may rise and fall in a periodic fashion or in one simple cycle. They may reach constant highs and lows, or may vary with inconsistency. Resistance, capacitance, and inductance vary endlessly with material electrical properties and length, size, and height above ground. But, they are bounded by maximum and minimum envelopes and the spreads, although large, are limited. In a shield room, standing waves on wiring may rise up at around 10 MHz.

Shield room resonance itself usually is around 50 MHz depending on size. On a large transport aircraft, resonance may occur around 1 MHz and continue into the higher frequencies. The fuselage may resonate at 1 MHz, the wing and other structural details at higher frequencies.

In a balanced transmission line circuit, resonance is kept to a minimum; signal stability and quality are maintained.

Single wires and braids (at their resonant frequencies in the 10s and 100s of MHz) offer very high impedances. A 40-inch, or 24-inch, or 9-inch wire or braid at 70 MHz (the VHF range) may have an impedance that has risen to 10 kΩ. A 4-inch long braid or a #20 wire exhibits about 500Ω at 100 MHz, roughly the same frequency range. With this kind of impedance increase and resonant condition, adding a wire connection between a circuit and ground may alter the surrounding field strength levels by 10 or 20 dB. The significant consideration here is that they are not stable conductors. As soon as appreciable capacitance and inductance are added, conductor quality is lost in a single wire or braid.

In unencumbered space, radio frequencies behave linearly, constantly, and predictably. Introduce conductors, metallic planes, and a range of materials, resistance, and dielectrics; and vary the structure, cabling shape orientation, and location; then only modeling and measurement techniques can focus on and map the radio frequency fields with any accuracy and reliability.

Even though there is a wide range of variation in the HF-VHF radio frequency region, the testing and measuring is performed in an equivalent shield room, metallic environment, complementary to the aircraft fuselage metallic environment. Increased field strengths from resonant and reflection activity in the shield room have been a rough emulation of the final installation.

### 4.1.2. Magnetic and Electric Field Distribution

From the 400-Hz powerline, those ubiquitous, unidentical twins, electric field and magnetic field, although easy to contain or block, nevertheless crisscross the length and breadth of today's aircraft and are present in every bundle and on every circuit. The magnetic field permeates all materials. It may couple to other wires. A wire with 4A may cause noise voltages up to 400 mV (figure 4.1-9) depending on wire length. These noise voltages can mar the signal fidelity in the input circuitry of analog sensors, passenger entertainment, radio headsets or interphones. The electric field charges all materials. It can induce high voltages. A 100-ft wire with 160V peak, 115V rms, may induce over 100V peak (figure 4.1-10) onto high-resistance circuits. These noise voltages will pester operational amplifiers or comparator circuits, although they will ignore low-resistance analog or digital signal drivers.

These twin marauders, almost always together, are st'engthened with increasing bundle length and encouraged by proximity of common wire routing. The magnetic field and electric field induced voltages of figures 4.1-9 and 4.1-10 have been plotted together on figure 4.1-11 and shown with the added variable of wire separation - the other dominant wire coupling parameter. See in figure 4.1-11 how the induced voltage drops with wire separation.

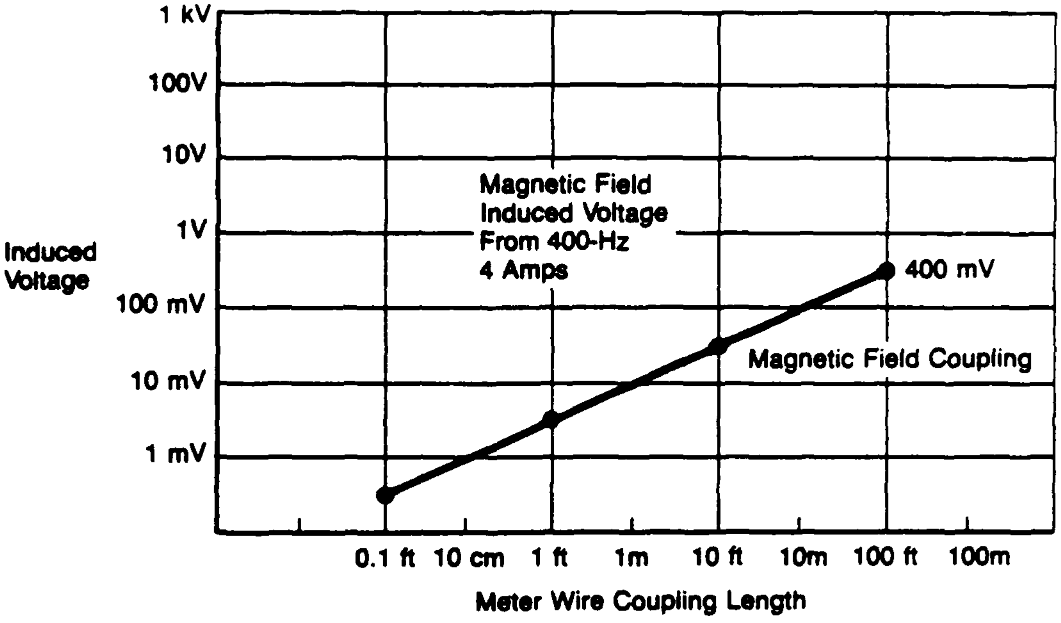


FIGURE 4.1-9. "H" FIELD COUPLING

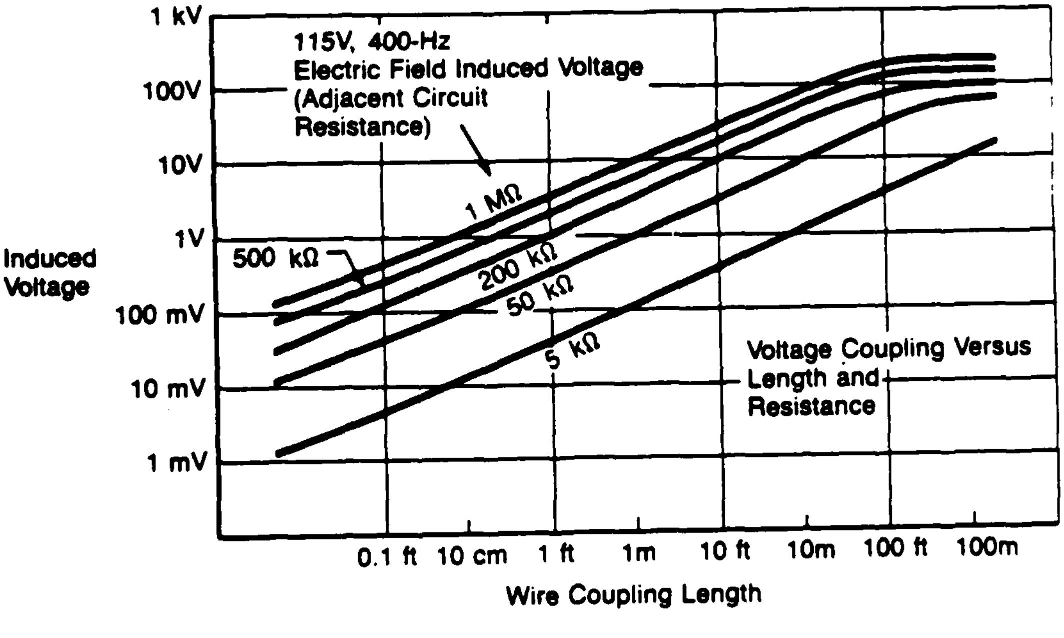
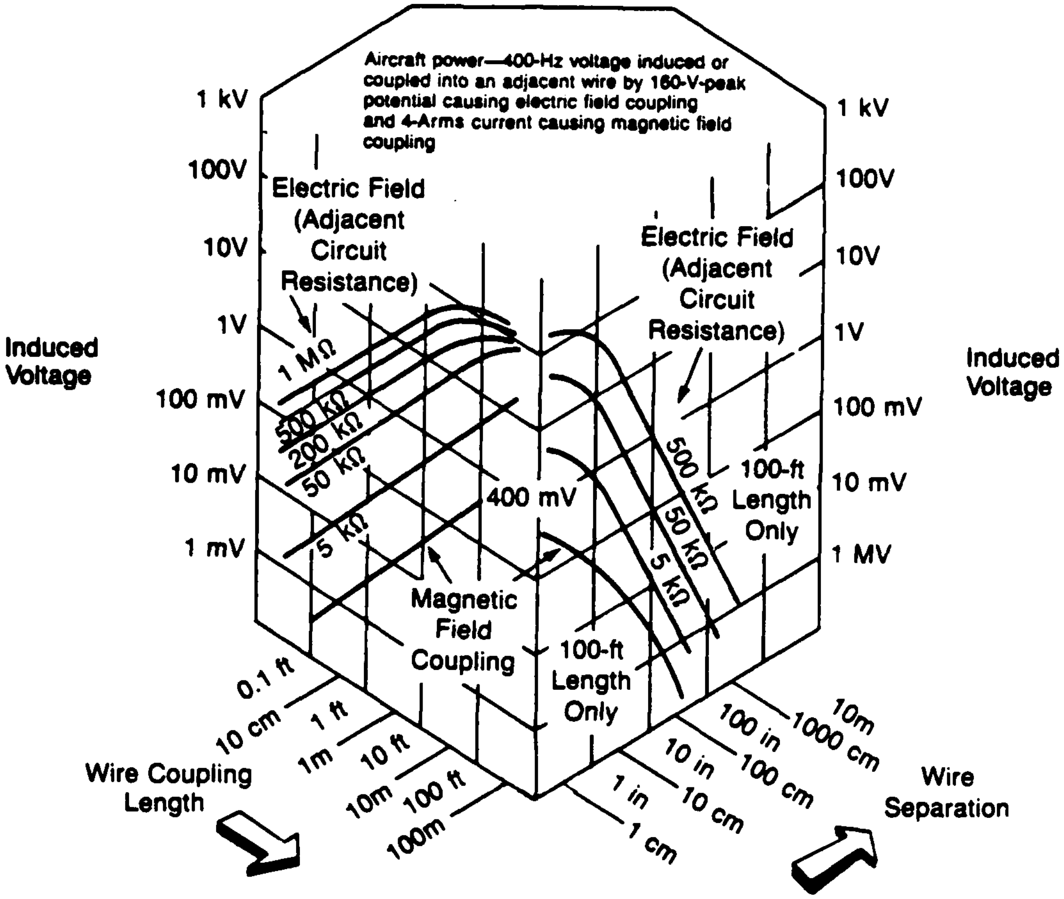


FIGURE 4.1-10. "E" FIELD COUPLING



Aircraft power—400-Hz voltage induced or coupled into an adjacent wire by 160-V-peak potential causing electric field coupling and 4-Arms current causing magnetic field coupling

FIGURE 4.1-11. COUPLING VERSUS SEPARATION

Now, there is one exception to the design panacea of using a twisted pair, shielded circuit as the perfect defense against electromagnetic interference. On present day aircraft, a circuit, even though it is twisted pair, will be subject to magnetic field induced voltages if it has a shield and the shield and circuit are grounded at both ends. (Aluminum aircraft structure carries the 400-Hz power line return currents. The 400-Hz current will thus travel in shields grounded at both ends. The shield current then transfers a voltage to the internal circuit.) A balanced isolated circuit design or double shielding will compensate. The first twin, magnetic field, induces voltages on other wires in a bundle, but it also radiates out from the bundles into the aircraft interior space and into equipment (figure 4.1-12). The radiated magnetic field emanating from the power lines varies in field strength from microgauss to gauss (milliamps per meter to amps per meter). The fields are of interest when flight-deck CRT displays, hand-held transceivers, and microphones (whose operational functions rely on the use of magnetics for control or display processes) are present. The magnetic field will easily cause distortion or "banding" on display tubes or will develop the sound of a 400-Hz "hum" in a speaker. Magnetic fields drop off in magnitude very rapidly with distance.

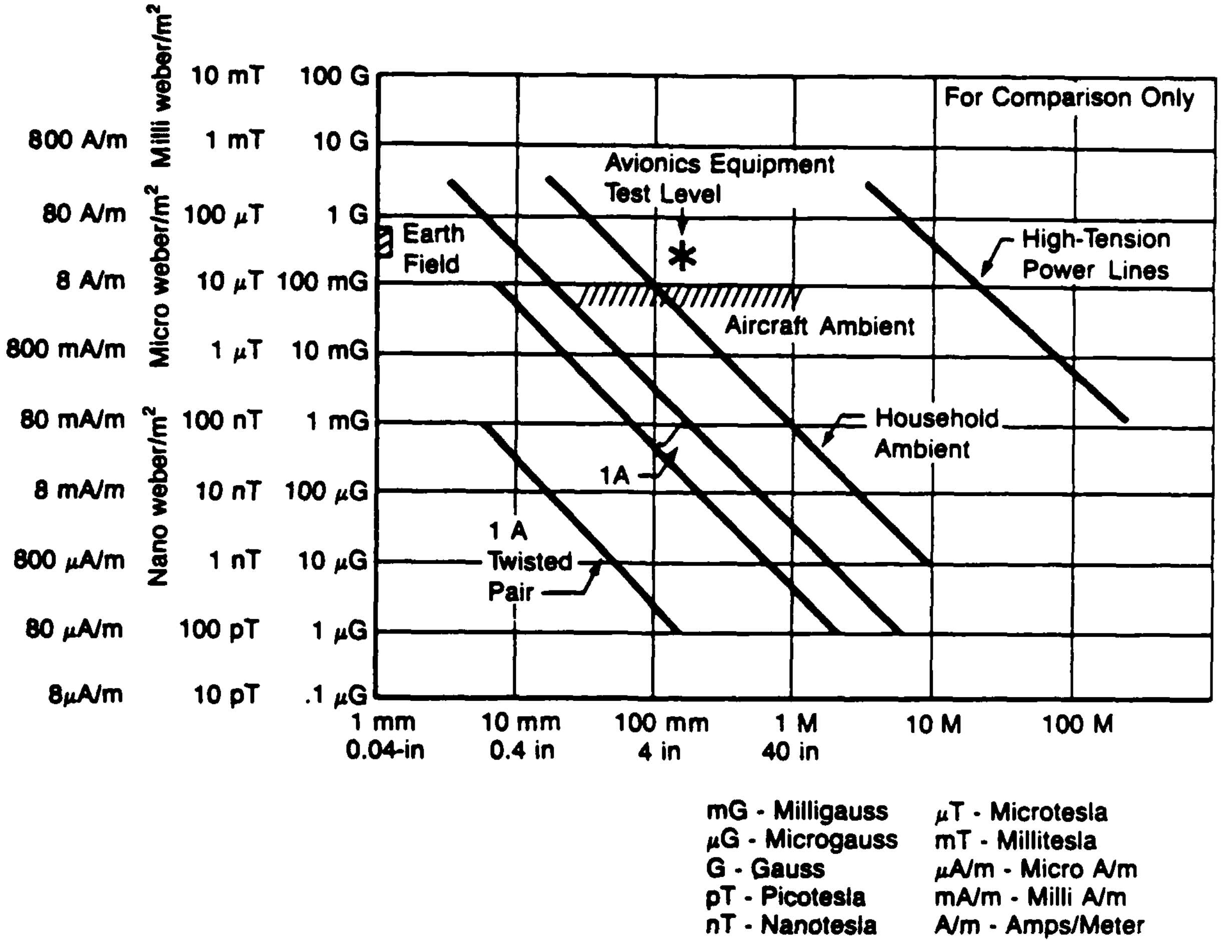


FIGURE 4.1-12. MAGNETIC FIELDS

The second twin, the 115V electric field from 400-Hz power lines, is in almost every aircraft cable bundle. The power line wire has a 115V rms (160V peak) potential. Another wire circuit brought into proximity of the 115V wire holds the 115V potential unless it is destroyed by the "electrical resistor divider" action of a low resistance on the adjacent or "victim" circuit. Figure 4.1-11 shows the reduction of voltage with reduced resistance on the adjacent circuit. The resistance is the parallel resistance of source and load. Either a low resistance or a shield will stop electric field coupling.

Careful attention to wiring details and design such as the use of twisted pair wire, shielding, balanced circuits, or fiber optics helps protect the aircraft against electric and magnetic fields.

### 4.1.3. Transients

A 115V power line supplying an inductive load, when interrupted by the opening of a switch or circuit breaker, will create an electrical switching transient often called an "inductive switching transient" or a "relay-induced transient." Electrical switching transients from lights, fans, pumps, or control surface actuator operation reach levels of 600V. Their duration can be over 1 ms, and their rise times nanosecond to microseconds. They harbor repetitive ringing waveforms or pulses (figure 4.1-13). These recurring ringing frequencies span the 1 to 10-MHz range. The switch opens, an electrical arc is started, and an inductive coil unloads stored energy through the arc in repetitive pulses onto a wire - a wire that may be bundled with other circuits carrying digital data or analog signals. The high-frequency energy is transferred capacitively and inductively to those circuits and directly into the internal harnessing and etched circuit card traces and microcircuits of an avionic unit. The electrical transient distributes to microprocessor clock, timing, or data lines.

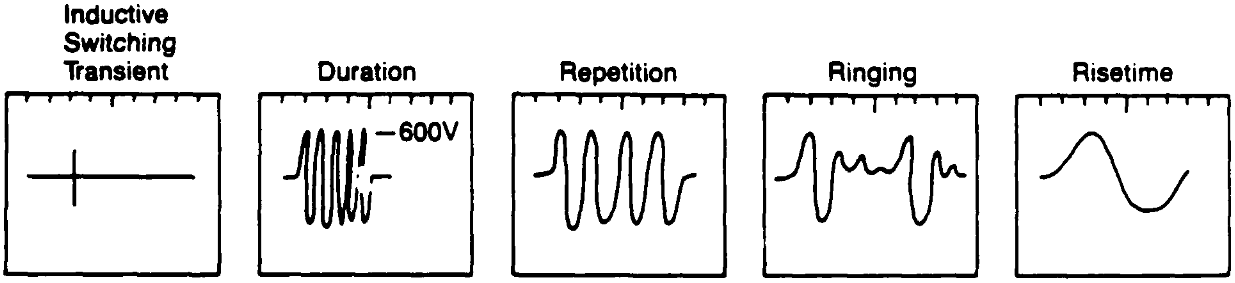


FIGURE 4.1-13. TRANSIENT RINGING

Very extensive measurements have been made of transients and their characteristics. L. Bachman states in his 1981 report: "This paper summarizes the results of the most comprehensive study ever conducted of U. S. Navy shipboard power line transients. Transient data was acquired on 13 ships - over 9400 hours of monitoring time - 2300 transients were encountered." Figure 4.1-14 is a summary. This study is remarkable in its extent and completeness. These transients show very similar, if not identical, characteristics of magnitude, risetime, and duration to those measured on commercial aircraft. In contrast to the high-level, inductive switching transient, the power bus may also experience momentary power interruptions, where the voltage drops to zero for as long as 50 ms.

Electrostatic discharge is another form of transient that can suddenly erupt under the right conditions of humidity, air or fluid flow, and juxtaposition of materials. Electrostatic discharges have much higher voltages - up to and over 10 kV, but much narrower pulse widths, possibly a 100-ns duration. A person on a dry Arizona-like day touching an avionic unit may discharge 10,000V onto the housing or wiring.

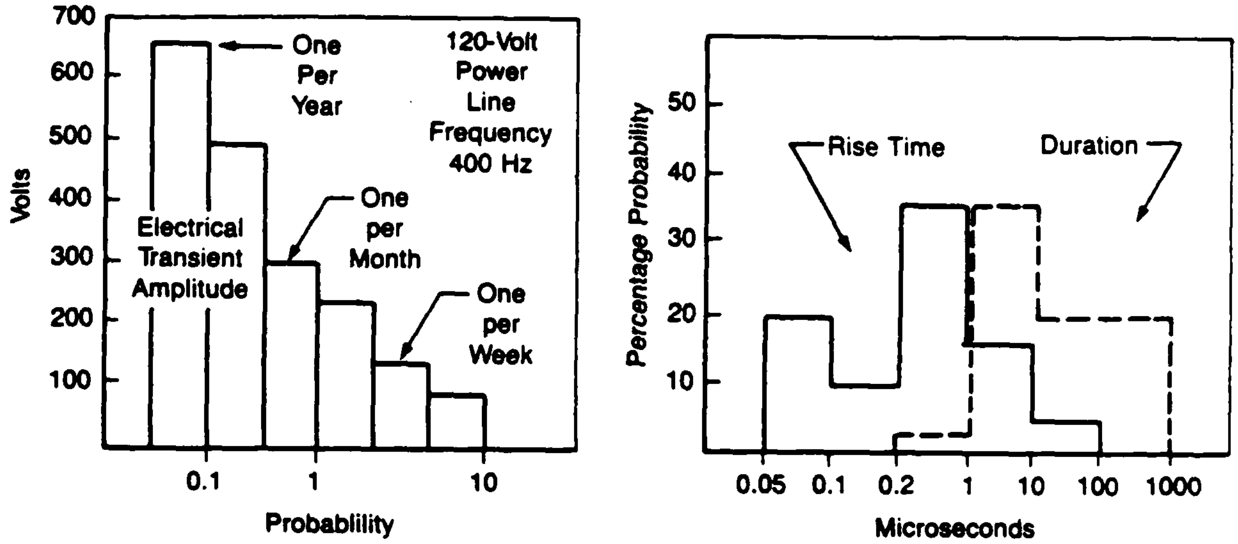


FIGURE 4.1-14. ELECTRICAL TRANSIENTS

One of the most evident electrical discharges, of course, is lightning. Large currents flow on the wing structure, fuselage, landing gear, or empennage leaving induced voltages in unprotected circuits. These induced voltages have resonant behavior often established by the characteristic of the size of the aircraft and length of wiring. Lightning protection is engineered to divert and contain voltages and currents in metallic structures to avoid damage to electrical wiring and parts. The transient voltage levels induced in wiring are required to be less than 600V. Induced voltages are usually less than 200V for the most severe strikes.

So you see, HF-VHF radio frequencies, 400-Hz power, and the various transients are electromagnetic interference or noise forms that are freely distributed and transferred into microprocessors to affect aircraft performance unless constrained and controlled by carefully integrated wiring and avionic and structure design.

## 4.2. Aircraft Protection

### 4.2.1. Shielding and Ground Reference

Aircraft and circuit protection is formed in a layered design: 1st layer, structural shielding, liners, trays, overbraid; 2nd layer, circuit shield; 3rd, balanced, isolated circuit; 4th, voltage, current limiting; and 5th, software.

Double shielding (two layers of shielding) fends off lightning and radio frequencies. For critical circuits having exposed wiring, double shielding is necessary.

Structure, skin, and panels of the aircraft form the first major level of shielding, and it is the system level barrier. Fuselage shielding is extended into open sections or unshielded areas, such as leading and trailing edge or landing gear, with a cableway, overbraid, or foil (figure 4.2-1). Shielding and wiring for radio frequencies, electrostatic charge, and lightning, safety fault returns and ground reference all call for a highly conductive material. Liners can be installed in nonmetallic electronic bay sections. Where spar, skin, or panel shielding is not inherent in structure, then foil, metal spray, or metal mesh (figure 4.2-1) can be designed into or onto nonconductive parts. Leading and trailing edges, engine bays, wheel wells, bulkheads, tail sections: all need evaluation to delineate the shielding and ground planes. Nonconductors, composites, and graphite-epoxy are not a ground or current return.

The second level or layer of shielding is individual circuit shielding continued (with back-shells) to the avionics enclosure shield. The second level offers protection against external threats and internal noise in wiring bundles too. The second level is connected, "grounded," to the first level.

### 4.2.2. Apertures and Electrical Bonding

Conductive panels, foil, or paint form and continue the shielding enclosure on skin panels and trays and, unless electrically bonded, will develop harmful voltages or electrostatic charge centers. (See excellent reports in bibliography by L. O. Hoeft on shielding and aperture losses.) Often good continuity is provided by fasteners. External items are electrically bonded and grounded to provide static discharge paths. Conductive paint is applied to external nonconductive surfaces.

Everything is searched out to check resistance.

- Materials: titanium, steel, stainless steel, aluminum alloys, fiber glass, graphite-epoxy, Kevlar, phosphor bronze, composites.

- Parts: instrument panels, keyboards, switching panels, seats, frames, window films or mesh, quick access doors, skin panels, cowls, fairings, trays, overbraid, backshells, plumbing, brackets, covers, control surfaces.

- Liners: foil, mesh, plating, depositions.

- Finishes: alodine, anodize, iridite, organic applications, copper plating, tin, silver, nickel.

- Sealants: paint, film, special substances.

Bonding is detail work, and often research and development is needed on new materials and techniques. Materials and procedures are recorded in a bonding and corrosion prevention document.

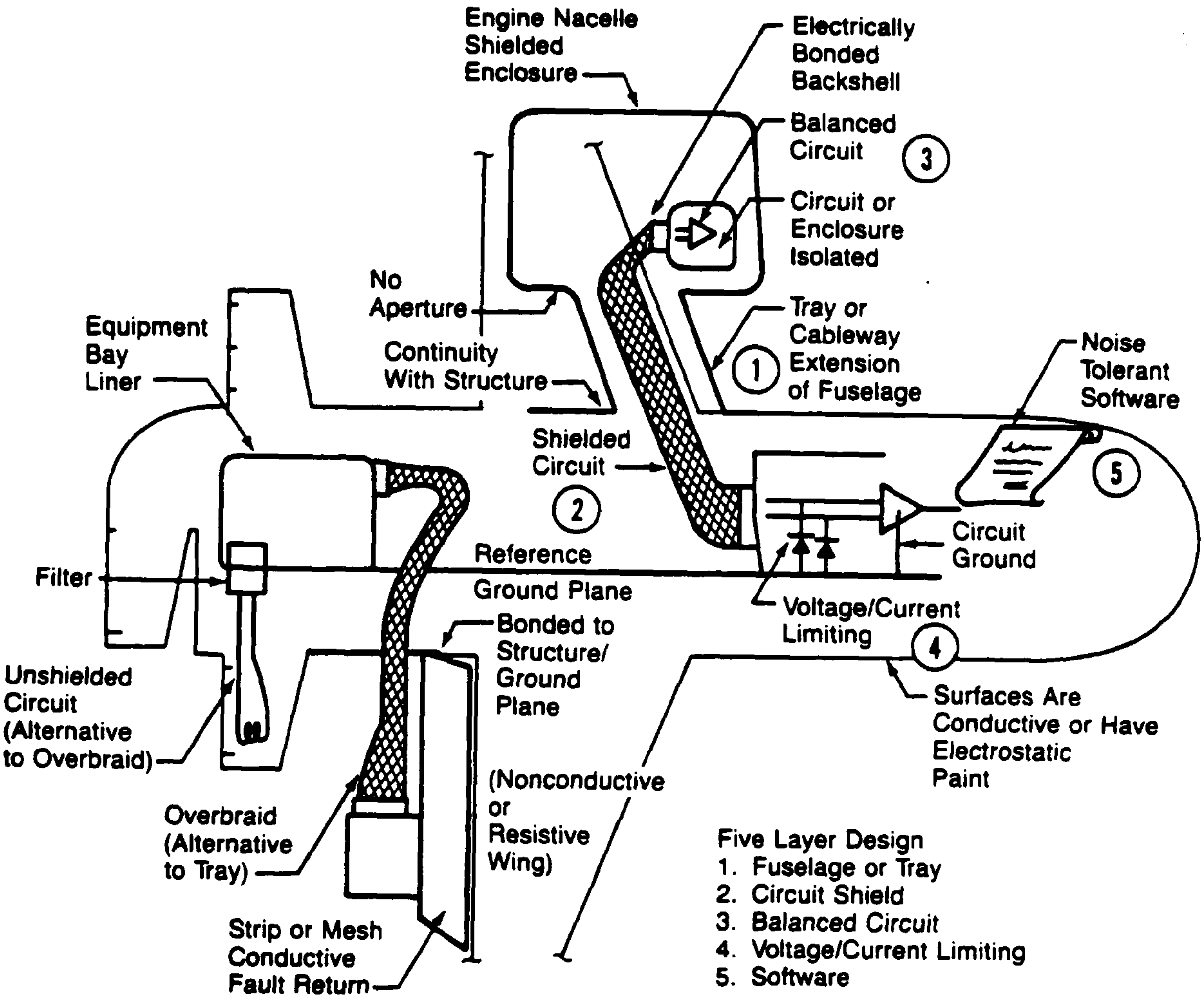

Engine Nacelle Shielded Enclosure
Electrically Bonded Backshell
Balanced Circuit
3
Circuit or Enclosure Isolated
No Aperture
Tray or Cableway Extension of Fuselage
1
Noise Tolerant Software
Equipment Bay Liner
Continuity With Structure
Shielded Circuit
2
5
Circuit Ground
Reference Ground Plane
Filter
Voltage/Current Limiting
4
Bonded to Structure/ Ground Plane
Unshielded Circuit (Alternative to Overbraid)
Surfaces Are Conductive or Have Electrostatic Paint
(Nonconductive or Resistive Wing)
Overbraid (Alternative to Tray)
Strip or Mesh Conductive Fault Return
Five Layer Design
1. Fuselage or Tray
2. Circuit Shield
3. Balanced Circuit
4. Voltage/Current Limiting
5. Software

FIGURE 4.2-1. LAYERED DESIGN

### 4.2.3. External Wiring Interface Circuits

Long wiring runs extending out to the wing and to the engines are unintentional antennas that collect noise. Data, control, and sensor lines, outside of the shielding of the fuselage, demand protection against radio frequencies impinging on engine struts or mounts, leading and trailing edges, and landing gear.

Engine instruments, pressure, temperature, speed, thrust control, air data, fire, flight control computers (circuits for actuators and control surfaces), proximity switches, position indicators, temperatures, and braking circuits are candidates for analysis and protection. Circuits are categorized by criticality. Line replaceable units may number from 50 to 100 units and digital buses, 200 to 300, but the buses will reduce to 30 or so different types with only 5 or 10 types being external to the fuselage. Future systems may have less than 10 digital buses. Discrete circuits number 30 or 40 different types, with around 10 external. They can be thoroughly analyzed.

Good rules for external circuits (there are exceptions):

Grounding:

- Circuits isolated from structure at exposed end.
- EMI tests applied to returns/grounds of units not on a ground plane.
- Primary to secondary power isolated.

Bonding:

- Case bonded to ground plane (when circuits isolated from case).
- Case isolated from ground plane (when circuits grounded to case).
- Backshell/connector bonded to case.

Shielding:

- Double shielding installed on transmitter lines.
- Internal shield grounded internally.
- External shield grounded externally (to backshell).

Input/output:

- Interface circuits balanced; clock and data signals routed together.
- Interface circuits isolated: transformer, LEDs, fiber optics.
- High resistance (greater than 10 kΩ) designed into circuits.
- All circuits filtered.
- No shared power wire returns.

Wiring/packaging:

- Return wire twisted with signal wire.
- No wires installed across an aperture (apertures bonded).
- Line drivers/receivers packaged close to connector.
- Connectors on equipment case placed in one local area.

### 4.2.4. Circuit Protection

Protection depends upon electronics design, packaging and, especially for external wiring, the voltage stress conditions: stress on insulation, thin films, integrated circuits, and trace spacing, Solenoids and motors with heavy insulation and no electronics usually do not require protection. Thin film and integrated circuits do. (See comprehensive reports in bibliography by R. L. Carney, R. A. McConnell, and D. L. Sommer for excellent treatment of protection devices.)

Every interface circuit needs analysis and voltage/current limiting. Naturally, the transient or radio frequency threat must be known; first define the open circuit voltage; second the surge or characteristic impedance of the wiring and the input impedance of the input capacitor, resistor, or diode; then determine short circuit current; and finally the transient time and energy, or radio frequency power. The following are variable, but important, voltage withstand requirements or test levels that apply to insulations, parts, and electronics and are usable benchmarks.

No protection usually required:

- 1500V rms, 2100V peak, 400-Hz signal, impressed for one minute; this is the voltage withstand specification for insulation (solenoids, motors).

- 3000V or greater, one microsecond transient withstand for insulation, varies with humidity, configuration, altitude, time.

- 1500V one microsecond transient, discrete resistor (molded part).

- 1500V fifteen mil circuit card spacing (at sea level).

Protection required:

- 200V or less, thin film, transient withstand voltage.

- 200 to 800V receivers protected by integrated circuit diodes.

- 100V transistors.

- 30V or less, operational amplifier receiver.

- 360V or less, fifteen mil circuit card trace spacing, at 100,000 ft.

- 360V or less, corona initiation at 100,000 ft, varies with shape.

The five layers of protection: (1) structural shielding, overbraid, cableway; (2) circuit shields; (3) balanced, isolated circuit; (4) voltage/current limiting; and (5) software combined with a stable ground reference plane help to guarantee compatibility.

## 4.3. Trades

It is critical to know program design requirements-and the environment. Dissect the electromagnetic topology of the aircraft including digital transmission, power system, and antenna fields. Round up new and off-the shelf equipment and bay locations. Search out aircraft structural and skin panel materials. Define the exposed critical circuits and equipment.

1st Major Trade: Location of equipment, categories, and tailoring of electromagnetic compatibility requirements of each unit. The wiring and the equipment is kept shielded under aluminum or graphite-epoxy and away from radio frequency fields (figure 4.3-1). Units of a subsystem collocated in a protected environment may have the design/test levels eased: lowered for susceptibility, raised for emission. Units not on the wing will not experience resonant conditions. Off-the-shelf equipment is often unchangeable at the input/output interface, and if located internally may save on shielding or externally mounted filters.

2nd Major Trade: Wire length and separation. Shortened wiring or elimination of wiring. Equipment location, equipment combination and wiring deletion are waiting for evaluation, for example, on-engine electronics supplied with on-engine power; major interfacing units physically located close together. Noise amplitude is proportional to length. Metallic wiring may be replaced with fiber optics to save tens to hundreds of pounds and 25% to 50% reduction of wires (figure 4.3-2) and major reduction of EMI.

3rd Major Trade: Digital, balanced, isolated circuits versus analog circuits and single-ended or discrete circuits. Delete or reduce open wiring. Reduction of wiring, shielding, transformers, power, weight through use of multiplexed digital bus (figure 4.3-3).

4th Major Trade: The five levels of layered protection. If structure shielding is not available, the following alternatives may be investigated. Trade cableways, overbraid, and exposed wiring with filter/voltage/current limiting. For one or two wires on noncritical circuit, filter may trade off better than overbraid or cableway.

A recent large program relied on the fuselage for the major portion of circuit shielding. Wheel wells, engine bays, outer wing sections, and radome areas were shielded. Quick access is often necessary. Overbraid (20% of the bundles) was installed for critical flight control circuits to "extend" the airframe. It was indicated in that design that the use of metal overbraid on all bundles might be 10 times heavier than reliance on the fuselage. Also, complexity of the topology limited the use of overbraid, and in certain areas a combination of protection was needed. For circuits inside the fuselage, filter pins were used; for outside circuits, voltage limiters. Discrete filters for each circuit were not pursued because of excessive volume and weight.

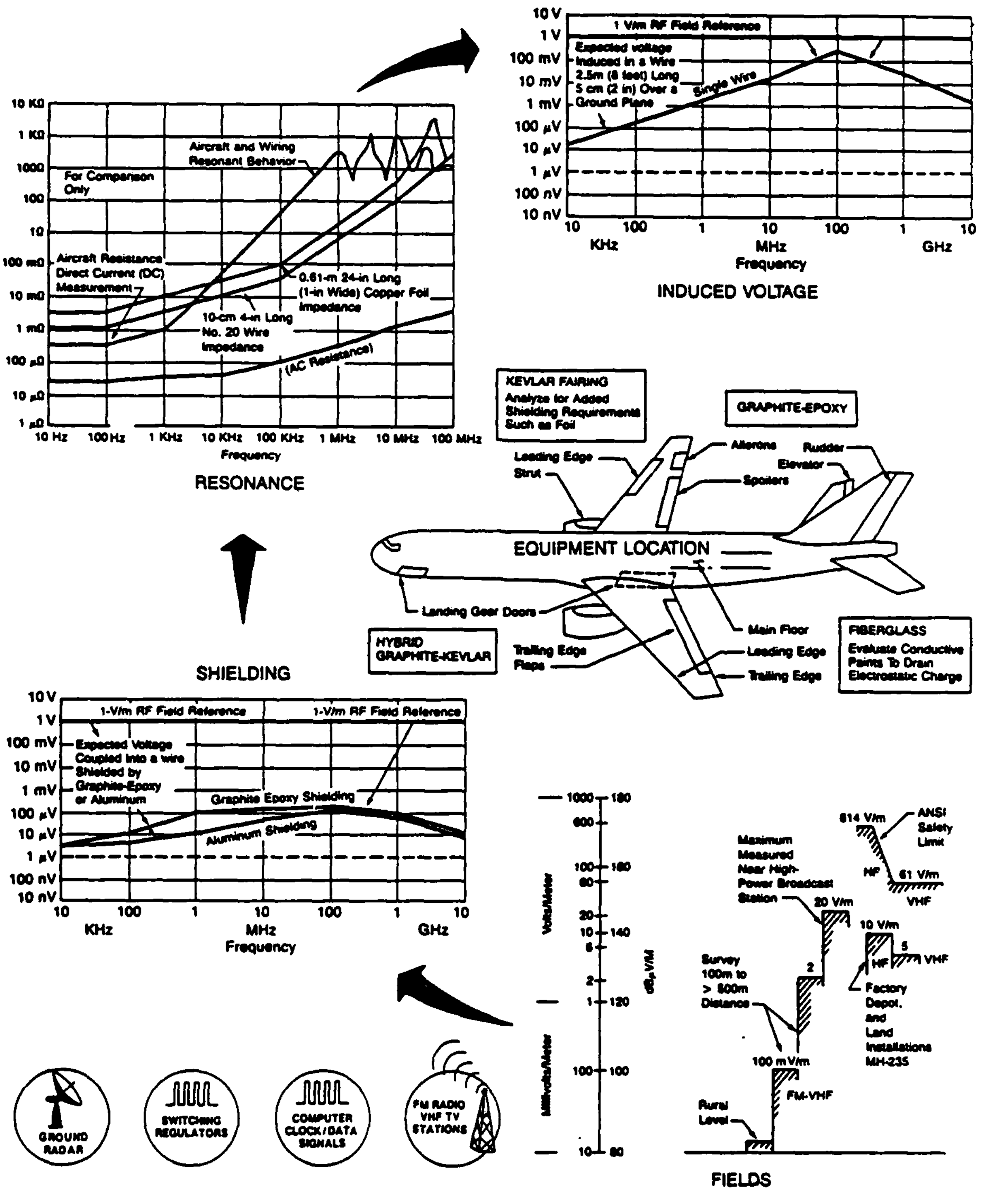


FIGURE 4.3-1. TRADE-EQUIPMENT LOCATION

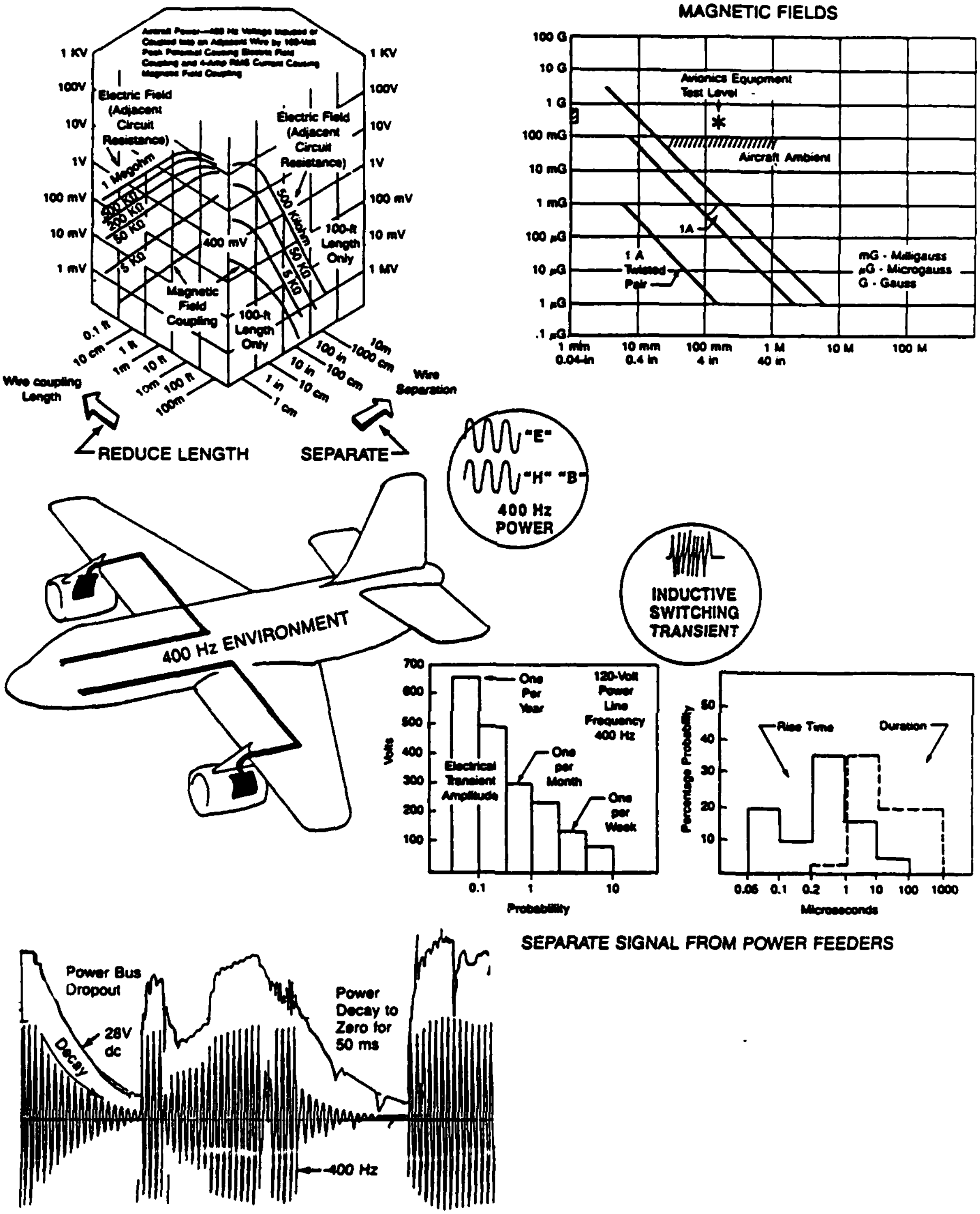


FIGURE 4.3-2. TRADE-WIRE LENGTH/SEPARATION

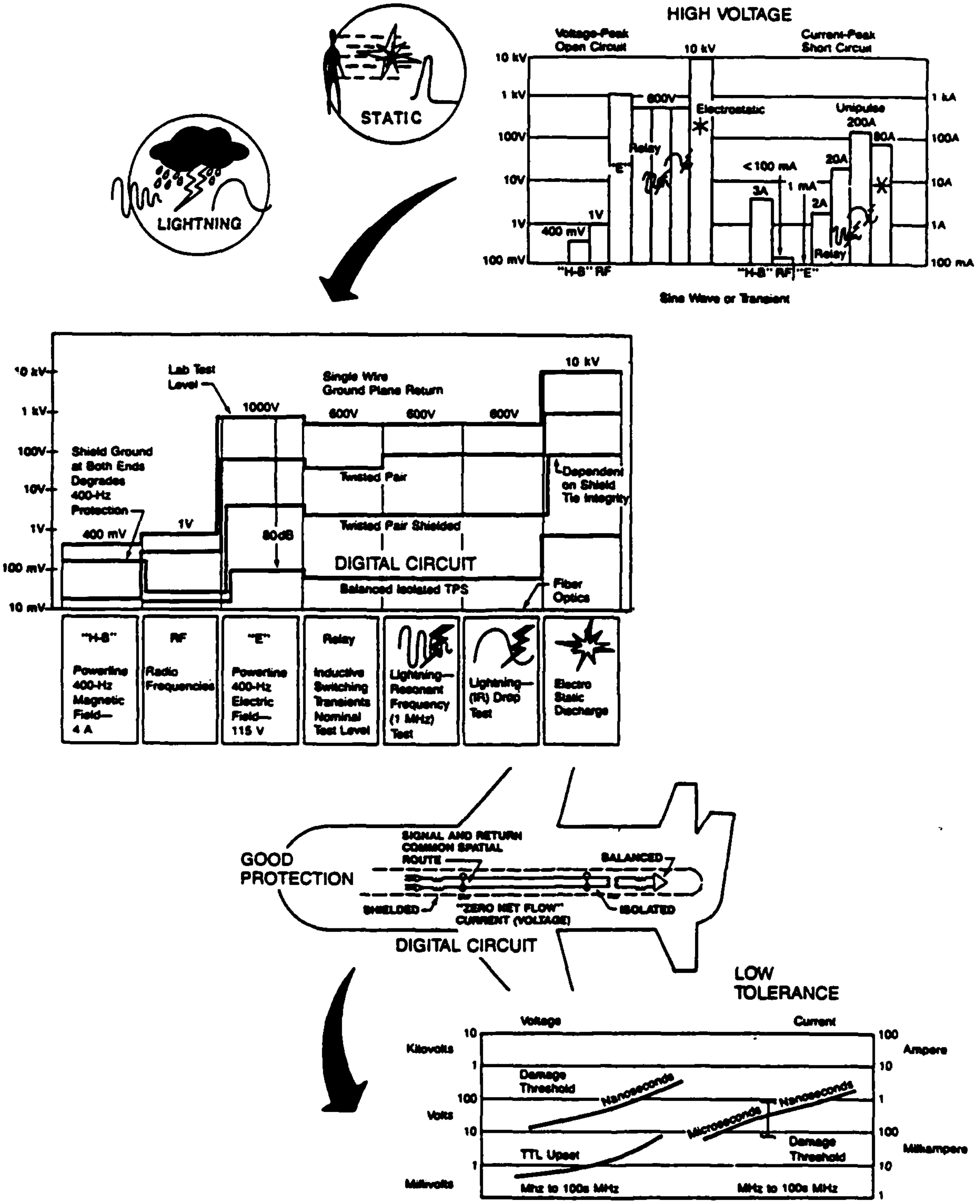


FIGURE 4.3-3. TRADE-DIGITAL CIRCUITS

If it is at all possible to install a cableway, tray or liner, it may be better in the long run. Consider these facts in favor of a tray:

Design:

- Proven designs/models and in-service experience.
- Easily formed, integrated with structure.
- Fewer electronics and "sneak paths".
- Freedom from reliability studies.

Protection:

- Line replaceable units installed with known protection.
- Freedom from frail electronics.
- Excludes high voltages and arcs.
- Rugged and durable.

Test:

- Lower test levels on electronics.
- Freedom from complex verifications.

Life cycle cost:

- Reduced engineering, part control, troubleshooting, maintenance.
- Easy in-service monitoring.
- Long life.

Computerized design procedures will speed the capability to make trades.

# 5. ACTIVITIES AND DOCUMENTS

## 5.1. Specifications/Documents

Some have postulated that most of the electromagnetic compatibility designs and trades at the airframe manufacturer's level must be quickly accomplished before go-ahead or at least at the very beginning of the program, that is: all of the major specifications must be set up - the equipment located and categorized - the environment documented - procurements contracted.

This may not, however, be as extensive an effort as it sounds because most specifications for environments and existing technologies are already available from other programs and need only to be reworked, shaped, and adapted.

Specifications set guidelines-standards-requirements. They are the foundation for any program, and a path that provides a reference and continuity. They help bypass unproductive squabbles and unnecessary changes. They sidestep duplication: "Reinventing the wheel?" They even help tie into the next program.

From the top documents, which outline the intent and scope, down to the lower tier designs, look for these specifications:

Industry:

- FAA Code of Federal Regulations, Aeronautics and Space #14, Parts 1-59; Part 25 Airworthiness Standards: Transport category Airplanes, reference 25.1309, 25.1353, and 25.1431; Part 23 Rotorcraft, 23.1309; Part 27 General Aviation, 27.1309.
- RTCA/DO-160B "Environmental Conditions and Test Procedures for Airborne Equipment," July 20, 1984, sections 1 to 3, and 15 to 22.
- (A generic industry system specification here would be appropriate.)

Program:

- "Program System Specification": Simple one or two paragraph delineation of top EMC references, generic system requirements, or scope.
- "System Electromagnetic Compatibility Design Requirements": Organized sections of system and aircraft program requirements for external environment, equipment categories, interface circuit policy, grounding, bonding, shielding, wiring, isolation, electrostatics, aircraft shield policy, special analyses, applicable EMC document list, and policy for critical equipment.

- "Equipment Electromagnetic Environmental Requirements Specification": Explicit equipment level design and test requirements including test setup and conditions-patterned after the industry standard DO-160.

- All Procurement Specifications: Reference in the design section to the "Equipment Electromagnetic Environmental Requirements Specification?" List of deviations. Requirements for power, dielectrics, circuit interfaces, grounding, bonding, shielding. Table of tests. Statement of Work: Developmental analysis and breadboard test report, analysis of off-theshelf equipment, technical exchange meetings, qualification test plan and report.

- Design Handbook/Guidelines/Design Notes: Interpretation and conversion of program design and test requirements into protection techniques.

- System Test Plan: Test policy and outline. Subsvstem tests. Aircraft tests: ground test, environment test, electrical bonding measurements, power switching test, flight test.

Related specifications:

- "Power and Electrical Requirements Specification": Aircraft and external ground power quality, returns and grounding design.

- "Wiring and Shielding Design and Manufacturing Procedure": Wire separation, shield construction.

- "Electrical Bonding and Corrosion Prevention": Materials, compatibility, *fasteners*, *surface preparation*, joining and sealing.

5.2. Tasks/Activities

At the beginning of the program, some participants think immediately of the analytical tasks and modeling. Some think of staffing, organization, and people. Others think of schedules. The EMC engineer must pursue the design; he thinks of what the new aircraft is: new materials, new equipment, old equipment, size, layout, wiring runs. Defining the aircraft for electromagnetic compatibility is a monumental effort. The effort cannot be delayed. It must be done quickly. Some details will not be available. There are roadblocks, but these are the engineering tasks.

- Identify in a table or spreadsheet all equipment: new and off the shelf; in-house and vendor; supplying agency; purchasing specification number. List the equipment versus applicable EMC requirements (including outmoded EMC limits), deviations, waivers, and approvals.

- Assess aircraft and equipment architecture: flight deck, electronic bays, externally mounted units, engine units, power and signal circuitry. Identify each equipment and installation and focus on grounding, bonding, shielding, materials and wiring.

- Set up electromagnetic compatibility design categories/groups.

- Track down procurement specifications: remove or add limits and EMC interfaces; establish the developmental, engineering model, qualification, and acceptance tests; communicate with Procurement, Project, and the subcontractor.

- Define topology, field patterns, power of transmitters, and dig out the receiver thresholds.

- Extract power system type, power quality, ground returns and ground points.

- Chase down aircraft advanced technologies and materials. Unearth the differences from past programs.

- Dissect the new environments, external and internal, that are different from DO-160.

- Document new test equipment needs.

With the aircraft definition in hand, the electromagnetic compatibility engineer can take each of the EMC program documents and cut and fit them together: no overlap, no deficiencies, just acceptable coverage. He tailors the requirements based on: (1) past experience, (2) new environments and technologies (3) equipment location, (4) critical circuits, (5) weight, volume, and (6) test. Important: aircraft specifications are finalized more easily before formal design release has been invoked.

Analysis cannot wait. Analysis and models feed on physical dimensions: fuselage-wing-landing gear, length, width, height; and electrical parameters: resistance, capacitance, inductance. Computer models are bringing new capabilities for quick evaluation of multiple design alternatives, and keyboard editing speeds the rapid reevaluation and turnaround when changes are proposed.

The apertures, seams, wire routing, overbraid, isolation, and the shielding effectiveness of aluminum, titanium, graphite-epoxy, and steel must be known along with interface protective designs that must be pulled out of the schematics: filter pins, discrete filters, balanced circuits, transformer isolators, fiber optics. Getting an early handle on these items expedites the many wire coupling and radiation analyses of common noise sources, for instance: power frequencies and ripple; pulse width modulated power; transients from solenoids, valves, motors; and clock oscillator harmonics.

Just a word about responsibility. The electromagnetic compatibility engineer is usually responsible for either a system and product or, conversely, for a technology or even a combination of both. Becoming knowledgeable in a technical area is often the best. For example, for technology:

- Computers/digital circuits software.

- Radio frequency transmitters, receivers, antennas.

- Power quality, generators, switching regulators.

- Analog instrumentation, transducers, sensors, fiber optics.
- Grounding/bonding/shielding/wiring/packaging.
- Dielectrics, corona, and materials.

And for example, product or system:

- Environmental control and cargo (power).
- Flight control/management (digital/software).
- Communication/navigation (radio frequencies).
- Power and lighting and fuel.
- Air data, flight instruments (video, analog, CRTs, displays).

The definition and specification of electromagnetic compatibility on an airplane program is a sporty task. It must be initiated early. Most airplane programs need at least three engineers. Future programs with advanced avionics and flight control systems may require four or five.

# 6. EQUIPMENT SPECIFICATION

## 6.1. New and Existing

The countdown is on until the specifications on every last unit of new and existing equipment are found, cut apart, organized, and set straight. Equipment "procurement specifications" are the bottom line. They define design and test requirements and waivers or deviations. If a unit meets its tailored, allocated electromagnetic compatibility specifications, then electromagnetic compatibility on the aircraft is almost always assured. Deliberate on and wring out every last detail:

- Tailored requirements for each unit (per RTCA/DO-160B).

- Each bonding/grounding/shielding interface (between the supplier and airframe manufacturer).

- Power quality specific requirements.

- Dielectric voltage withstand levels.

- Circuit interface wiring design.

- Detailed unit tests: developmental, engineering model, qualification, acceptance.

The specifications on new and existing units give exact requirements, item by item, on electrical and physical parameters and tolerances.

Existing equipment has already proven itself with its "in-service history," and treatment is different from new equipment. Existing equipment is addressed with attention to conformance to past specifications and any new program requirements. On a new program, old requirements may not be adequate: transients may need redefinition and reapplication depending on unit location; electric field protection may need to be increased; radio frequency susceptibility tests may need strengthening; and power bus momentary interruptions may be a problem. Development tests cannot be overemphasized for new and even existing units. The policy is "make it upset" in order to find margins. Development tests are important and are a major element of successful programs. EMI protection cannot be competently added after the finalized design.

The packaging engineer and circuit designer at the supplier have to know the overall design policy for new and old equipment. They must also know what their interface design is going to be. Key design requirements may be dispersed in various documents but should be either in a system specification or in the equipment procurement specification. Policies or requirements vary from program to program, product to product; these are some standards:

Grounding:

- Designed, controlled, equipotential ground plane system.
- Optional digital circuit ground to case.
- No analog (audio) circuit ground to case without approval.
- Primary to secondary power isolation (transformer electrostatic shield).
- Power single point ground system; "star" architecture.
- No power current in nonmetallic structure.
- EMI requirements apply to returns/grounds of units not on ground plane.

Bonding:

- Case bonded directly to ground plane or,
- Connector pin for case ground wire.
- Backshell/connector bonded to case.

Shielding:

- Internal shield grounded internally.
- External shield grounded externally (to backshell).
- Shields grounded at both ends (except analog).
- No circuit current on shield (except coax).
- Double shield on transmitter lines.

Input/output circuits:

- Interface circuits balanced; clock and data signals routed together.
- Interface circuits isolated; transformer, LED, fiber optics.
- Increased circuit power ratings at outputs.
- Return wires run twisted with the signal wires.
- Connector pin for circuit ground.
- Connector pin for case ground or fault wire.
- Voltage/current limit all interface circuits.

- No shared power returns.

Packaging:

- Separation/isolation of power from signal.
- Power, signal, and ground returns on separate pins.
- Line drivers/receivers close to the connector.
- High-frequency circuits close to the connector.
- Low-frequency circuits at back of the box.
- Connectors on equipment case placed in one local area.

6.2. Aircraft Equipment Categories.

Category definition needs immediate attention. Avionics must not be over or under designed. Equipment categories represent the modification and tailoring of DO-160 requirements to units of equipment having widely variant properties or environment:

- Computers, power generators, transducers, motors.
- Units with extra long interface wiring.
- Units placed on or off the aircraft ground plane.
- Equipment exposed or not exposed to high-energy radio frequency.

Here are some typical categories:

Category 1A:

Energy storage devices (having no electronics): inductors, valves, motors, solenoids, and relays switched continuously or automatically. The items in this category are designed and tested to conducted emission and radiated emission requirements only. They do not require susceptibility tests.

Category 1B:

Energy storage devices operating on an intermittent basis, less than once every three minutes. The conducted emission and radiated emission requirements are raised (relaxed) 20 dB.

Category 1C:

Energy storage devices having short duration transients and operating two times or less per flight. Emission and susceptibility requirements are waived.

Category 2A:

Electrical/electronic equipment: avionics, power equipment, any unit having electronics located within the fuselage and protected by the fuselage metallic structure. All of the standard equipment electromagnetic compatibility requirements, equivalent to DO-160, apply: conducted emission, radiated emission, conducted susceptibility, radiated susceptibility.

Category 2B:

Electrical/electronic equipment within the fuselage, but having long wiring runs, over 100 ft. All standard requirements apply along with a raised (possibly 3 dB) 400-Hz electric/magnetic field and radio frequency field tests.

Category 2C:

Transmitters/receivers: All standard requirements, and with antenna terminal conducted emission and susceptibility tests added.

Category 3A:

Electrical/electronic equipment outside the fuselage and well shielded, but exposed to higher lightning induced transient activity. All standard requirements plus lightning induced transient requirements.

Category 3B:

Electrical/electronic equipment unshielded under nonconductive material or on external mountings. All standard requirements apply and lightning plus increased radio frequency susceptibility test levels (possibly 100 V/m).

Category 3C:

Electrical/electronic equipment not on a ground plane. All standard requirements apply and susceptibility and emission requirements are also applied to the equipment circuit ground, power ground, and case ground interface wires.

Category 4:

Support equipment associated with the aircraft. Apply radiated emission and conducted emission requirements on power that connects to aircraft.

Category 5:

Flight-test equipment: Apply radiated emission requirements and radiated susceptibility requirements for external equipment. Flight equipment is isolated from aircraft circuits.

## 6.3. Suppliers

Early in the program the EMC engineer hastens to know the supplier (vendor or subcontractor). It is important to record and establish a file of equipment identification, electrical characteristics and the tailored requirements:

- Unit: name, acronym, model, unique identifications.
- Company: name, location, engineers, organization.
- Affiliated paper: procurement specification, interface control drawing, statement of work, interface schematics.
- Unit history: new, existing, modified, previous program usage, in-service experience, equipment similarities, deviations, waivers.
- Schedule: technical meetings, prototype/engineering models, test dates, qualification test procedure.
- Grounds/bonds/shields: internal ground, interface bonding.
- Test: development, engineering model, qualification, acceptance.
- Subsystem: project engineer, staff engineer, contracts engineer.

At program startup, there may be specific candidate proposals and subcontractor control plans or procedures to evaluate. These are important attributes to look for:

- Treatment and awareness of specification requirements.
- Unit in-service use on previous programs.
- Past programs experience and success.
- Evaluation and analysis capabilities.
- Implementation of design techniques.
- In-house or provisions for testing facilities.

Of course, the size of the program will dictate the extent of the subcontractor effort, but this might be a typical statement of work:

> "The subcontractor shall conduct an early investigation and developmental EMC analysis and test on the breadboard or prototype hardware for new or modified equipment."
>
> "A developmental test report and evaluation shall be forwarded to the prime contractor containing information on noise measurements of interface circuits and proposed wiring, protection, and emission control techniques."

> "The subcontractor shall obtain available EMC data and in-service history on existing, off-the-shelf equipment; determine compliance with the program requirements; and, where requirements are not met, recommend options for equipment modifications, deviations, or waivers."
>
> "The subcontractor shall conduct timely technical exchange meetings and present grounding, shielding, hardware, and software protection. A qualification test plan and report shall be submitted for comment and approval."

The statement of work for the subcontractor may be more or less detailed depending on complexity and size of the equipment or subsystem.

Subcontractor equipment design changes are made throughout the entire program. An EMC engineer cannot monitor or assess all engineering changes on all equipment, but a change involving electrical properties may require some reevaluation or retest. For example, anytime a change deals with new coupling characteristics, that is: wiring harness rerouting, new input/output circuits, different circuit board layout, extensive software modification that changes timing sequence or adds new loops, then an analysis or susceptibility retest is appropriate. The vendor maintains complete responsibility and accountability for design and test verification of his unit or subsystem to fully utilize his own facilities, experience, test equipment and software capabilities.

# 7. VERIFICATION AND VALIDATION

## 7.1. Key EMC Designs

Verification: Equipment qualification test at a supplier to prove that a design meets specification. The qualification test of equipment forms the very keystone of verification.

Verification is also accomplished in the airframe manufacturer's laboratories to prove performance of key EMC designs and properties, such as:

- Grounding of digital or analog circuits.
- Bonding resistance of aircraft part, wire, or joint.
- Shielding properties of new materials.
- Leakage of joints and apertures.
- Emissions of pulse width modulated power.
- Wiring design and coupling conditions.
- Aspects of aircraft mounted filters and limiters.
- Susceptibility thresholds of interface circuits.

Verification tests quickly lead to the ultimate proper operation on the aircraft. Measurement reveals thresholds and noise upset margins. Verification lays a groundwork before validation.

Validation: Demonstration of and confidence in proper equipment function along with acceptable control of noise during aircraft operation in its intended environment.

Demonstration - A two part measurement and test:

- Operation of an aircraft (or subsystem) through its normal modes while operating equipment and devices.
- Introduction of jeopardizing noise environments to stress equipment: all the while monitoring functioning flight deck instruments and aircraft circuit operation internally and externally: internally with built in test circuits/equipment (BITE) and externally with meters, transient recorders, oscilloscopes, spectrum analyzers, and digital bus analyzers.

An airplane program must be structured on a foundation of solid verification and validation (see section 9).

## 7.2. Validation Plans

First, hasten to collect, document, and rely on existing qualification data, existing validated technologies, and validation by similarity.

Otherwise, validation tests can be run at the subsystem level in a flight avionics laboratory or on the production aircraft.

When considering subsystem versus aircraft test, assess the following deficiencies and benefits in cost, effectiveness, flexibility, and timeliness:

TABLE 7.2-1. SUBSYSTEM VERSUS AIRCRAFT TEST

| | | | | | |
|---|---|---|---|---|---|
| COST: | CAPITAL EQUIPMENT | ATTENDANT PERSONNEL | EQUIPMENT REWORK | TEST EQUIPMENT | LEARNING CURVE |
| Subsystem | Very Low | Low | Low | Low | Low |
| Airplane | High | High | High | High | High |
| ENVIRONMENT: | EQUIPMENT COLOCATION | RF SIMULATION | GROUNDS/ SHIELDS | RESONANT CONDITIONS | |
| Subsystem | Poor | Good | Poor | Different | |
| Airplane | Actual | Good | Actual | Actual | |
| DESIGN: | FINAL HARDWARE | FINAL SOFTWARE | TEST SOFTWARE | FINAL WIRING | ENGINEER AVAILABLE |
| Subsystem | Good | Good | Excel | Fair | Good |
| Airplane | Excel | Excel | Excel | Actual | Fair |
| PROCEDURE: | APPROVAL SIGNATURES | FORMAL SEQUENCE | DECISIONS/ DIAGNOSTICS | CHANGE CONTROL | PROGRAM TIMING |
| Subsystem | Few | No | Best | Good | Fair |
| Airplane | Many | Yes | Fair | Good | Late |

Aircraft offers fidelity, but demands a high price with inflexibility in a dedicated airplane outfitted with test equipment. The avionics laboratory is an active testing and simulation facility and testing can often be done speedily on a "noninterference" basis when test time is slack. Circuit access panels already exist. Testing can be easy, informal, flexible and promote diagnostics and real-time knowledge of noise behavior. A range of tests can be run at the subsystem level with selected tests on the aircraft.

## 7.3. Validation Procedure

The subsystem or aircraft configuration, setup, test equipment, and modes are identified and recorded paragraph by paragraph for each separate mode. The procedure then records step-by-step operation of equipment.

CONFIGURATION: Model, make, serial numbers, outstanding engineering changes or deviations, wiring or customer configuration, software, test software, test date, location.

TEST SETUP: Equipment bay lights, test stands, ground planes, shield ties, ground wires, unique simulations, monitors.

TEST EQUIPMENT: List test equipment and installation for the following systems by paragraph section:

- Flight control/flight management: computer breakout boxes, digital bus analyzers, oscilloscopes.

- Communication/navigation: interphone electronics breakout boxes, receiver breakout boxes, interphone headsets, RF voltmeters, spectrum analyzer.

- Power: power supply breakout boxes, chart recorders, transient analyzers, peak reading (transient) voltmeters.

- Flight indicating/recording: flight instrument breakout boxes, digital bus analyzers.

- Engine: monitors, indicators.

- Environment: magnetic field measuring instruments, spectrum analyzer and current probe (wiring) and antennas (radiated emission), signal generators.

PERSONNEL: Knowledgeable subsystem or equipment engineers, experienced EMC engineers and technicians. Monitor and record all initial settings, indicator light status, measurement instrumentation, BITE readouts. On functioning displays, observe and record status of flight instruments, CRT panels on flight deck, left, right, and center control panels, power panels. During step-by-step procedure, record upsets, circuit breaker disconnects, state changes/events, autopilot disconnect, warning signals/flags, annunciations, CRT distortion on all subsystems.

SOFTWARE: Identify software installation and initiation for each mode. Automated test software routines exercise processing functions and interfaces and monitor the data, status, error counters, or fault logging in real-time or on printout.

MODES OR PRESETS: Establish modes and settings for all systems:

- Environmental control: pressurization, temperature, air control.

- Flight control/management: mode control panel, autopilot engage at "left or right command"; test software installation, flight management computer; control display unit, flight path program, takeoff, cruise, landing, autoland; engine control operation.

- Communication/navigation: ADF, HF, VHF, ATC transmit/receive frequency modes and settings, IRS navigation modes, selector panel interphone left and right settings.

- Power: circuit breakers engaged/disengaged.

- Fuel and hydraulics: pumps, valves.

- Flight instruments and recorders: flight instrument, caution/advisory readouts, recorders.

- Lighting: light settings, dimmers, strobes.

- Engine: electronic engine control settings, indicators.

- Degraded modes: loss of redundant unit, low battery.

FUNCTIONAL SWITCHING TEST PROCEDURE: Establish a step-by-step procedure paragraph for each mode and possibly for each major subsystem. For chosen mode perform "functional switching test?" That is: operate, switch on/off, cycle, or exercise all units:

- Environmental control: pressurization, temperature, fans.

- Flight control/flight management: motors, actuators, flaps, slats.

- Communication/navigation: HF-VHF transmit.

- Power: all circuit breakers.

- Fuel and hydraulics: pumps, valves, solenoids.

- Flight indicating/recording: flight instruments, CRTs, recorders

- Lighting: cabin, flight deck, strobe, and landing lights.

- Engine: electronic controls, indicators, actuators, indicators.

A subsystem or airplane EMC validation test procedure demonstrates the absence of malfunction or undesirable noise and authenticates that the repeatability, accuracy, and reality of operation in normal modes of an airplane baseline production configuration meets the Federal Aviation Regulations and the Aircraft System Specification.

ENVIRONMENTAL STRESS TEST PROCEDURE: Establish separate paragraph for each mode or subsystem as above and operate equipment while introducing transients or radio frequency energy. The policy is "make it upset" not "show success?" If noise is transient, vary the pulse repetition rates relative to computer processing control cycles. Equipment should operate within performance specification and also demonstrate:

- Maintenance of proper internal configuration.

- Successful automatic restart.

- Continued operation.

- No permanent faults.

- No adverse control surface motion.

- Automatic transfer to secondary systems.

NOISE MEASUREMENT: Measure and characterize the signature of noise on the digital data bus, communication circuits or cables, interphone circuits, powerline bus, analog instrument circuits, and in the aircraft ambient to assist in validating operation and establishing a data base for diagnostics, not only for the existing program, but for future programs. Establish a separate paragraph for each mode. The following are noise types or thresholds:

- Clock oscillator harmonics or HF-VHF transmitter signals on circuits and cables.

- ADF-HF-VHF threshold sensitivity; passenger address circuits, voice recorder, crew interphones noise and thresholds.

- Powerline switching transients at circuit breakers and equipment terminals, switching regulator harmonics on buses and on cables.

- 400-Hz electric and magnetic field strengths, HF-VHF field strengths.

BONDING RESISTANCE TEST: Measure resistance of structure joints, skin panels, electrostatic paints, liners, foils, doors, flight deck panels, strut fairings and wing.

Testing and test assessment rests so heavily on a product's history and the intent of the product's function and future use, that it is, of course, an individual or program responsibility to define test concepts, requirements, and procedures. This validation test information, therefore, represents possible guides or techniques, but must be considered as not being appropriate for a specific test.

## 7.4. Program Design Reviews

During a program there is no quicker way to help improve the validity and timeliness of the design and specifications than by periodic reviews to establish agreement on perceived requirements and outcome. The following items are for consideration and might be selected and presented in a program preliminary design review or critical design review to help lay groundwork for verification, validation and certification:

- Program documentation, organization.

- Aircraft system and RTCA/DO-160 design/test requirements.

- Environment assessment, equipment EMC categories.
- Subsystem, equipment architecture/topology.
- Grounding system plan.
- Bonding: radio frequency/static/safety.
- Shielding: aircraft and wiring
- Wiring design, critical circuits.
- New technologies analysis/models.
- Equipment/subsystem/aircraft verification/validation plan.

The prompt review of key documentation and requirements helps to start and keep the program on a successful path.

## APPENDIX A - TEST AND TEST LIMITS

Early EMC history has seen the radio receiver as the centerpiece of electromagnetic field testing. It was necessary to find the source of noise entering aircraft audio circuits and radios. The keys today, in measuring emission and susceptibility parameters, are the oscilloscope and spectrum analyzer; the need for noise control spread to instrumentation and automatic pilot circuits.

We are now seeing the need for digital logic analyzers, bus controllers, and automatic, interactive testing capability to measure performance in fly-bywire, negative stability, aircraft systems.

Spectrum analyzers and storage oscilloscopes are proven and powerful troubleshooting tools in the measurement of noise. The scope displays the analog time domain waveform. The spectrum analyzer lays out the frequency components of that waveform. The scope shows peak amplitude. The spectrum analyzer reveals amplitudes versus frequency. With a scope, the pulse repetition rate is measurable. And with the spectrum analyzer, harmonics are caught in any frequency band. But, although spectrum analyzers and digitizing oscilloscopes are useful in finding and characterizing noise, it is ineffective to apply them to the task of detection of errors or noise margins in computers. The EMC community now needs these units to be paired with high-speed data bus analyzers and logic analyzers in order to provide even simple measurements of computer processor operations, such as: timing sequence, state activity, and bus status.

Recently, the processing functions of an avionic computer were upset by noise causing the unit to suspend operation, to "lock up?" It then required recycling of power to restart operation. Personnel from the electromagnetic compatibility group were asked to help diagnose the unpredictable upsets. An oscilloscope (analog waveforms) and the spectrum analyzer (frequency components) displayed noise occurring on the wire returns, grounds, and logic power supply lines; the noise levels were high enough to interfere with clock and data signals; wavering clock timing pulses destabilized the processing sequences; noise and unstable signals appeared everywhere on the circuit boards traces.

Many days were spent on this problem, but with "analog" instrumentation a solution could not be found until logic analyzers and bus controllers were brought in. Without the capability to control data entry formats, observe and evaluate output activity, timing sequences, and to correlate state changes with noise events, timely solutions to complex problems become impossible.

Future validation testing on automated aircraft systems will require laboratory personnel to monitor simultaneously occurring events, to visually correlate timing, logic state changes, and to automatically record data, decoded and converted, in real-time under a number of aircraft modes. Digital interface bus analyzers, logic analyzers, and interactive computer controllers will offer fast solutions and bring about professional insights to noise problems on new digital avionics.

Laboratory personnel are called upon to execute a variety of tasks:

- Circuit research.
- Test equipment construction.
- Diagnostics and troubleshooting.
- Evaluation of avionics performance.
- Avionics and airplane qualification testing.

And laboratory personnel diagnose problems in a variety of aircraft units: computers, power controllers, transmitter/receivers amplifiers, motors/generators, analog sensors, all of which encompass a wide range of characteristics. Functions of the aircraft, in a flight context, span the systems of environmental control, flight control, flight management, fuel, communication, navigation, power, and engine controls, but to the EMC engineer and laboratory technician these functions bring to mind susceptibilities and emissions:

- Power: 400-Hz, dc buses, motors, relays, switching events.
- Dc-to-dc switching regulators, pulse width modulation controllers.
- Radio frequency receiver thresholds and transmitter antennas fields.
- Data transmission and clock oscillators.
- Sensitive analog (audio) sensors and circuits.

Data, information, and histories already exist on environmental levels and are documented in the RTCA/DO-160B and MIL STD 461 specification (see table A-1).

But, for noise effects on data, transmission and timing sequences relative to conditions of circuit stability and upset margins, the EMC community today does not have an adequate data base.

Speeds of future systems will increase, voltage levels will rise, and sensor and receiver thresholds will be lower and more sensitive. Emerging flat panel displays, microprocessor controls, voice controlled systems, dc power systems, and pulse width modulated, electric actuators will be available soon for full authority flight controls and will be beyond the reach of engineers in the EMC community for test and analysis.

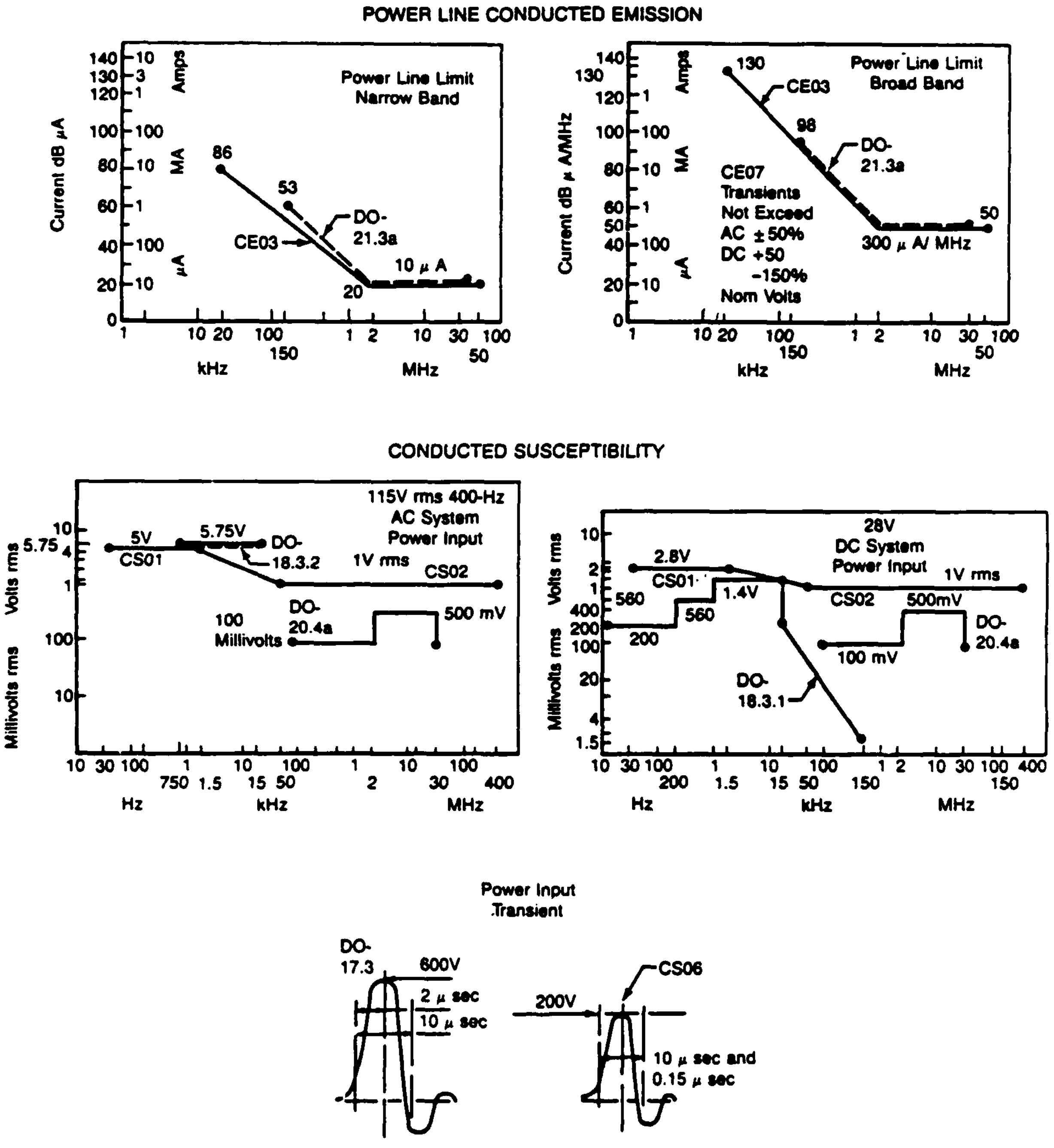
In the shield room, the controlled environment and standard electrical references (for instance, voltage, current, impedance, frequency meters, and ground planes) offer established laboratory conditions for analysis and tradeoffs of digital flight control designs. But, most of the time during today's EMI tests, current probe factors, antenna factors, line losses, attenuation factors, and bandwidth conversions are now essentially hand calculated and joined with raw data almost on a point-by-point basis in an anachronistic, time-consuming process. These computations are a hindrance, but the more important loss is inability to assess trends and compare, in real-time, circuit operational changes in a controlled and repeatable manner under various noise levels.

Controlling, probing, comparing, and recording status and data transmissions (being digital in nature) against the itinerant noise occurrences (having analog waveforms) stands or falls on the test and simulation capability.

Effectiveness resides in the technician's skill and his experience coupled with the tools and equipment with which that skill and experience is implemented. New, modern equipment having automatic microprocessor controls and automatic data readout is becoming available to provide interactive test decisions. Equipment and tools of the "analog" 1960s and 1970s cannot carry the load or be compatible with the flight controls of the "full-authority," "fly-by-wire" 1990s.

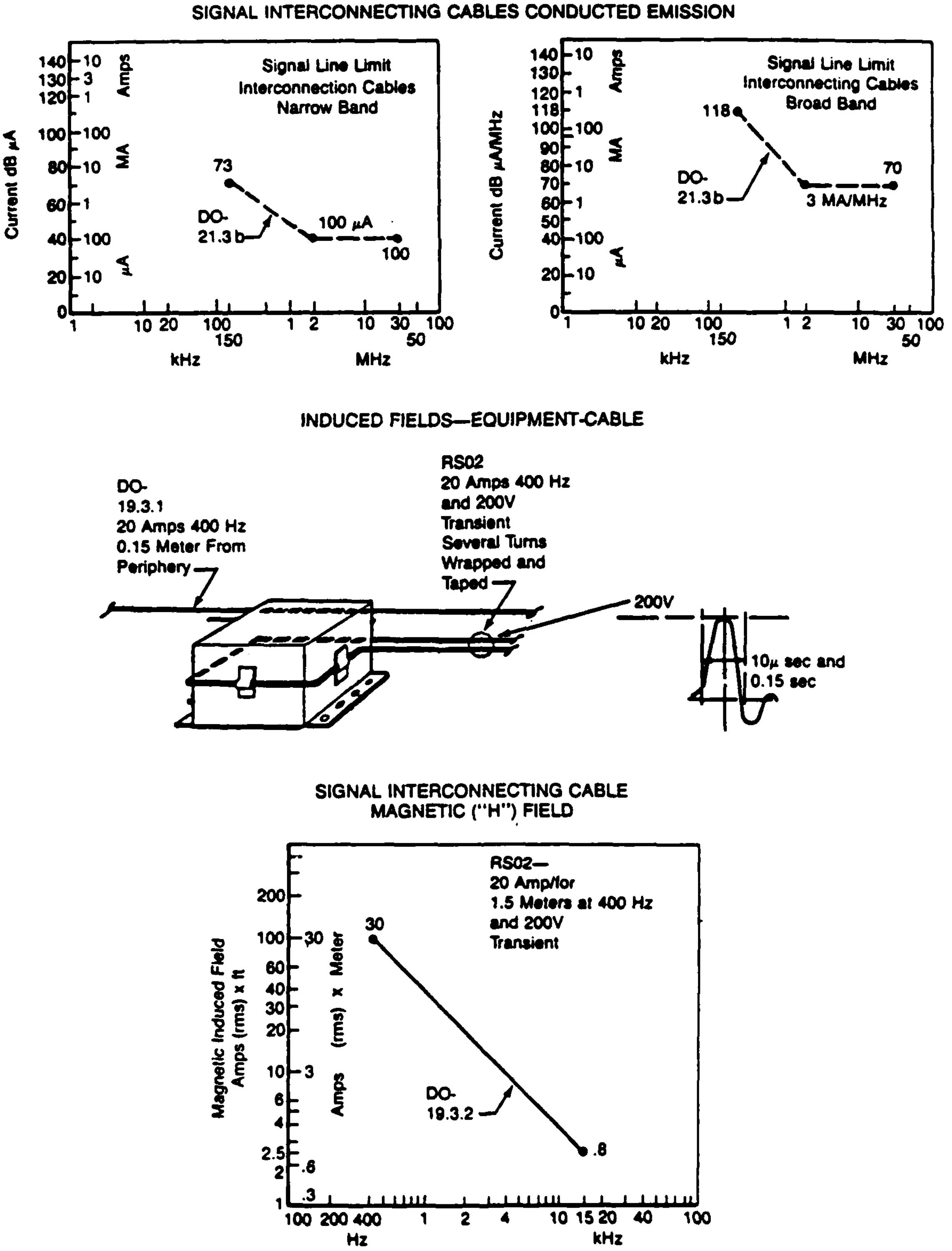
TABLE A-1. DO-160B AND MIL STD 461B. TEST CROSS REFERENCE
(see figure A-1)

| TEST | 160B | 461B |
|---|---|---|
| POWER BUS: | | |
| Conducted Emission | 21.3a | CE03 |
| Switching Transients CE | None | CE07 |
| Conducted Susceptibility (CS): | | |
| Audio Frequency CS | 18.3 | CS01 |
| Radio Frequency CS | 20.4a | CS02 |
| Power Line Spike | 17.3 | CS06 |
| Bus Momentary Interruption | 16.5.1.4 | None |
| EQUIPMENT AND SIGNAL CABLE: | | |
| Conducted Emission Cable | 21.3b | None |
| Induced into equipment and cable: | | |
| Magnetic "H" Field Equipment | 19.3.1 | RS02 |
| Magnetic "H" Field Cable | 19.3.2 | RS02 |
| Transient Spike: 200V | None | RS02 |
| Electric "E" Field Cable | 19.3.3 | None |
| Inductive Switching Transient | 19.3.4 | None |
| Radio Frequency CS Cable | 20.4b | None |
| EQUIPMENT & INTERCONNECTING CABLE: | | |
| Radiated Emission | 21.4 | RE02 |
| Radiated Susceptibility | 20.5 | RS03 |



Note: The "DO-" indicates the RTCA/DO-160B paragraph.

FIGURE A-1. EMI TEST LIMITS (1 of 4)



SIGNAL INTERCONNECTING CABLES CONDUCTED EMISSION

INDUCED FIELDS—EQUIPMENT-CABLE

SIGNAL INTERCONNECTING CABLE
MAGNETIC ("H") FIELD

FIGURE A-1. EMI TEST LIMITS (2 of 4)

## INDUCED FIELD—EQUIPMENT-CABLE (CONTINUED)

Electric Field

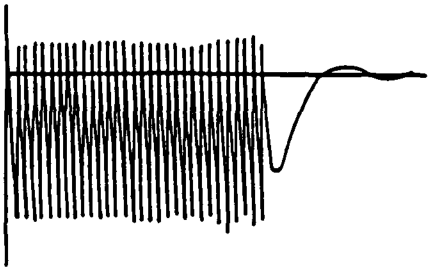
DO-
19.3.3
380 to 420 Hz
1800 Volt x Meters

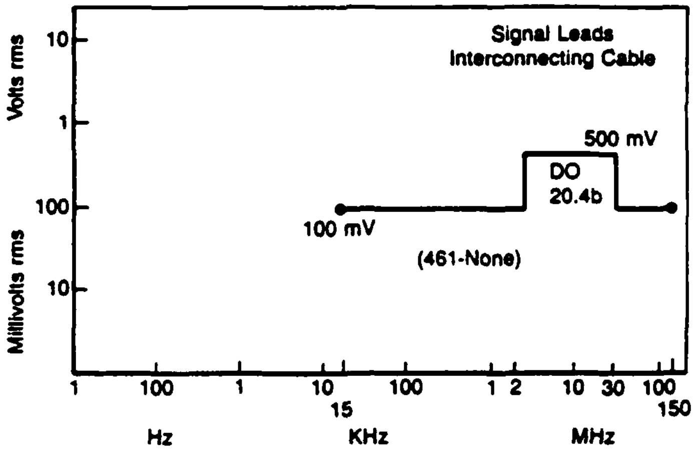
(461-None)

DO-
19.3.4
600 Volt Peak-Peak
8-10 PPS for 10 sec

(461-None)

Relay Transient





RADIATED EMISSION

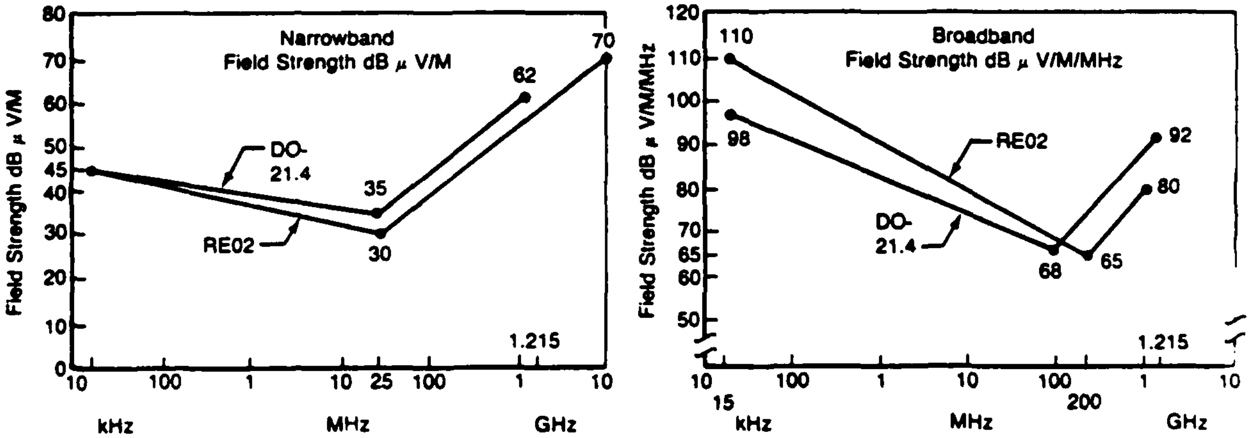
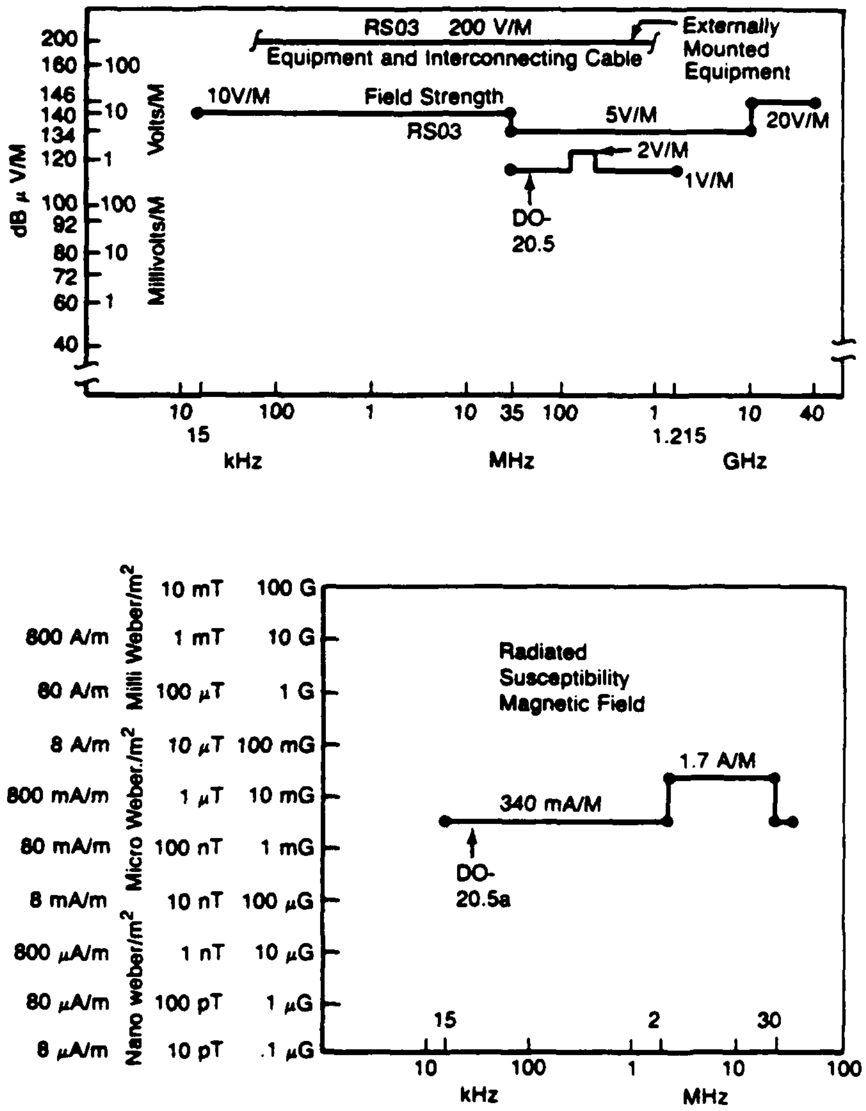


FIGURE A-1. EMI TEST LIMITS (3 of 4)



RADIATED SUSCEPTIBILITY

FIGURE A-1. EMI TEST LIMITS (4 of 4)

# BIBLIOGRAPHY

AC 25.1309-1, *Advisory Circular-Systems Design Analysis*, Federal Aviation Administration, September 7, 1982.

AFSC DH 1-4, *Air Force EMC Design Handbook*, January 10, 1972.

Ahmad, S., "Shielding and Aging Effects With Flexible Coaxial Cable," 1985 IEEE EMC Symposium.

Annanpalo, Jaakko, "Common-Mode Interference Rejection in Electrically Short Twisted Pairs," *EMC Technology*, September 1986.

ANSI C95.1-1982, "American National Standard Safety Levels With Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 300 Kilohertz to 100 Gigahertz."

ARINC 429-8, "Digital Information Transfer System (DITS)," October 31, 1978.

Bachman, L., "An Assessment of Shipboard Power Line Transients," 1981 IEEE EMC Symposium.

Baker, D. M., D-18306, *Magnetic and Electrostatic Wire Coupling in the Audio Frequency Range*, The Boeing Company, July 1956.

"Belden-Wiring and Shielding Data," *Belden Electronic Wire and Cable, Co.*, Richmond, Indiana.

Belisle, K. M., "EMI Design Techniques for De-coupling and Isolation of Microcircuits, 1983" IEEE EMC Symposium.

Biegon, R., "EMC Characteristics of RS-232 Cable Assemblies," *Connection Technology*, January 1986.

Birken, J. A., NAVAIR AIR-518-7, *Notebook on Electromagnetic Properties of Composite Materials Below 1 GHz*, September 1981.

Bly, R. P., "The Inside and the Outside Are Not the Same - Experimental Investigations of Ground and Shield Topology," 1982 IEEE EMC Symposium.

Boaen, V., "Designing Logic Circuits for High Noise Immunity," *IEEE Spectrum*, January 1973.

Bodnar, G. D., "Shielding Effectiveness Measurements on Conductive Plastics." 1979 IEEE EMC Symposium.

Brettle, J., "Electrical Bonding in Aircraft," 1979 IEEE EMC Symposium.

Brooks, P., Physical Design and Electronic Packaging Part 1, EDN, September 5, 1973.

Carney, R. L., D180-27423-49, Part IV "Design Guides for Air Vehicles," February 1987.

Chesworth, E. T., "Electromagnetic Interference Control in Structures and Buildings," EMC Technology, January-February 1986.

Clayton, R. E., "Transmission Line Electromagnetic Compatibility," 1975 IEEE EMC Symposium.

Code of Federal Regulations (CFR) 14, Part 25 Airworthiness Standards, "Transport Category Airplanes, Sub Part F Equipment:"

25.1301, Function and Installation
25.1309, Equipment, Systems, and Installations
25.1351, General
25.1353, Electrical Equipment and Installations
25.1431, Electronic Equipment

Cowdell, R. B., "Simple Equations Compute Radiated Emissions," 1983 IEEE EMC Symposium.

Crawford, M. L., "Comparing EM Susceptibility Measurement Results Between Reverberation and Anechoic Chambers," 1985 IEEE EMC Symposium.

Creason, R. R., "Measurement of the Magnetic Field From Long Two-Wire Lines at Low Frequencies," 1983 IEEE EMC Symposium.

DeMario, W. F., "New World for Aerospace Composites," Aerospace America, October 1985.

Dillon, W. L., "Antenna to Antenna Analysis of the E-4A Advanced Airborne Command Post," 1974 IEEE EMC Symposium.

Ditton, V. R., "Coupling to Aerospace Cables at Microwave Frequencies," 1975 IEEE EMC Symposium.

Dixon, D. S., "Low Frequency Radiated Magnetic Field Emissions: Rationale for a MIL STD 461B, RE-01 Limit Change," 1984 IEEE EMC Symposium.

DOD-HDBK-263, Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices),"May 2, 1980.

D6-16018, Electric Bonding and Grounding Design Requirements, The Boeing Company.

D6-16050-2, Electromagnetic Interference Control Requirements, The Boeing Company.

Don White Consultants, Inc., DM-S81, "Syllabus EMC - Design and Measurement for Control of EMI," March 9, 1981.

Dubil, E. F., Electrostatic Discharge Special Supplement Douglas Service, Vol. 42, October 1985.

Final Environmental Impact Statement for Seattle City Light, Highline 230 KV Transmission Project.

ECAC Study, A320 Electromagnetic Environment (A320 EME), by IIT Research Institute, (Contract F19628-85-C-0071 prepared for Federal Aviation Administration).

Force, R. D., "Integrated Application of Active Controls (IAAC) Technology to an Advanced Subsonic Transport Project," ACT/Control/Guidance System Study-Volume I, NASA CR-165963, December 1982.

__________., Report D180-20186-4, Investigation of Effects of Electromagnetic Energy on Advanced Composite Aircraft Structures and Their Associated Avionic/Electrical Equipment, September 1977.

Gibbons, R., "Performance Analysis Helps Designers Fine Tune Software," Electronic Design, October 18, 1984.

Glancy, D., "Preventing EMI in ATE Systems," Test and Measurement World, January 1987.

Gormady, J., "Random Susceptibility of an IC 7400 TTL Nand Gate," 1983 IEEE EMC Symposium.

Hafer, J. W., "The Effects of Shield Grounding Techniques for Isolation to Electromagnetic Waves," 1981 IEEE EMC Symposium.

Hariya, E., "Instruments for Measuring the Electromagnetic Shielding Effectiveness," 1984 IEEE EMC Symposium.

Hart, A. R., LSI Design Considerations for ESD Protection Structures Related to Process and Layout Variations, Hewlett Packard Company.

Heirman, D. N., "Education and Training of the Industrial Regulatory Compliance Test Team," 1981 IEEE EMC Symposium.

Hitt, E. F., DOT/FAA/CT-82-115, Validation of Digital System Avionics and Flight Control Applications, December 1982.

Hjellen, G. A., "A Thermal Damaged Model for Bi-Polar Semi-Conductors," IEEE EMC Symposium.

Hoeft, L. O., "A Simple Theory for Predicting the Electromagnetic Performance of Enclosures," 1985 IEEE EMC Symposium.

__________., "Current Division and Shielded Conductive Cables," 1983 IEEE EMC Symposium.

__________., "How Big a Hole is Allowable in a Shield," 1986 IEEE EMC Symposium

__________., "Measured Magnetic Field Reduction of Copper Sprayed Wood Panels," 1985 IEEE EMC Symposium.

Jarrett, R., "Software Fault Tolerance Staves Off the Errors that Besiege Microprocessor Systems," Electronic Design, August 9, 1984.

IPC-D-317, "Design Standard for Electronic Packaging Utilizing High Speed Techniques," August 1985.

ITEM Interference Technology Engineers' Master, Robar Industries, Inc., R & B Enterprises Division.

Kashyap, S., "Feed Cable Resonance in a TEM Cell," 1985 IEEE EMC Symposium.

Kendall, C. M., DOT/FAA/CT-83/49, Aircraft Generated Electromagnetic Interference on Future Electronic Systems, December 1983.

__________., "Data Processing Grounding A Need For Circuit Isolation," 1982 IEEE EMC Symposium.

__________., "EMC Control in Mainframe Computing Systems," 1985 IEEE EMC Symposium.

__________., "Microfiltering of Input/Output Cables," 1978 IEEE EMC Symposium.

Ketterer, J. R., "The Navy F/A-18A Hornet Electromagnetic Compatibility Program," 1981 IEEE EMC Symposium.

Koeritz, K. W., "A Systems and Environmental EMC Control Program for the Airtrans Automated Ground Transportation System," 1974 IEEE EMC Symposium.

Larsen, W. E., IEEE Transactions on EMC, "A Modified Ebers-Moll Transistor Model for RF Interference Analysis," November 4, 1979.

__________, Paper No. 84-2605-CP, 6th DASC, "An Overview of the Digital Avionics Assessment Activities Being Conducted by the FAA at NASA-AMES," December 1984.

__________, DOT/FAA/CT-84/9, The Effect of Aircraft Generated Electromagnetic Interference (EMI) on Future Avionic Systems A Compendium, April 1984.

Liao, S. Y., "Light Transmittance and RF Shielding Effectiveness of a Metallic Film Coating on a Plastic Substrate," 1977 IEEE EMC Symposium.

Lowe, K., "Noise-margin Analysis Automatically Lays Bare Hidden Logic Problems," Electronic Design, October 18, 1984.

Madle, P. J., Cable and Connector Shielding Attenuation and Transfer Impedance Measurements Using Quadraxial and Quintaxial Test Methods, 1975 IEEE EMC Symposium.

March, D. N., "Siting Considerations for Industrial Facilities That Generate Environmental Electromagnetic Noise," 1980 IEEE EMC Symposium.

Martin, A. R., "Shielding Effectiveness of Long Cables," 1979 IEEE EMC Symposium.

McAteer, O. J., "Shocking Blow to Military Electronics," Military Electronics/Counter-Measures, June 1979.

McBrayer, P., "RF Compatibility-Environment to Component Part," IEEE EMC Symposium.

McConnell, R. A., DOT/FAA/CT-87/19, Contract NAS2-12448, Avionics System Design for High Energy Fields.

MIL-HDBK-235-1A, Electromagnetic (Radiated) Environment Considerations for Design and Procurement of Electrical and Electronic Equipment, June 23, 1972.

MIL-HDBK-35 (USAF), Management and Design Guidance Electromagnetic Radiation Hardness for Air Launched Ordinance Systems, January 15, 1981.

MIL-STD 461B, Electromagnetic Emission and Susceptibility Requirements for the Control of EMI, April 1, 1980.

MIL-STD 1250 (MI), Corrosion, Prevention, and Deterioration Control in Electronic Components and Assemblies, March 31, 1967.

MIL-STD 1553B, Digital Databus System.

MIL C 5541A, "Chemical Films and Chemical Film Materials for Aluminum and Aluminum Alloys," March 31, 1964.

Morgan, G. E., "Examples of System Engineering in the EMP Hardening of Facilities and Aircraft," 1983 IEEE EMC Symposium.

Morgan, M. G., "Power Line Fields and Human Health," 1985 IEEE EMC Symposium.

Moser, J. R., IEEE Transactions on EMC, "Peripheral Cable Shield Termination: The System EMC Kernel," February 1986.

National Research Council, Aeronautics Technology Possibilities for 2000: Report of a Work Shop, Aeronautics and Space Engineering Board, Commission on Engineering and Technical Systems, 1984.

Olsen, R. G., "A Simple Model for Weakly Coupled Lossy Transmission Lines of Finite Length," 1984 IEEE EMC Symposium.

Ott, H. W., "Digital Circuit Grounding and Interconnection," 1981 IEEE EMC Symposium.

Palmgren, C. M., "Shielded Flat Cables for EMI and ESD Reduction," 1981 IEEE EMC Symposium.

Paul, C. R., "Affect of Pigtails on Coupling to Shielded Wires," 1979 IEEE EMC Symposium.

__________., "Coupling of Electromagnetic Fields to Transmission Lines," 1981 IEEE EMC Symposium.

__________., "Prediction of Cross Talk in Flat Pack, Coaxial Cables," 1984 IEEE EMC Symposium.

__________., "Printed Circuit Board Cross Talk," 1985 IEEE EMC Symposium.

__________., "Sensitivity of Multiconductor Cable Coupling to Parameter Variations," 1974 IEEE EMC Symposium.

Regan, J. J., Plastics Technology, "EMI Shielding: What You Need to Know And Why," January 1980.

Rhoades, W. T., "Achieving ESD Equipment Protection With Emission Controls," 1985 IEEE EMC Symposium.

__________., "Designing Commercial Equipment for Conducted Susceptibility," 1979 IEEE EMC Symposium Records.

__________., "Development of Power Main Transient Protection for Commercial Equipment," 1980 IEEE EMC Symposium.

RTCA/DO-160B, Environmental Conditions and Test Procedures for Airborne Equipment, July 20, 1984.

Schneider, L. M., "Noise Source Equivalent Circuit Model for Off-line Converters and Its Use in Input Filter Design," 1983 IEEE EMC Symposium.

"Shielding Against Electromagnetic Interference," Plastics Design Forum, March/April 1979.

Shimayama, T., "Measurement of the Suppression Characteristic of Filter Network," 1984 IEEE EMC Symposium.

Shores, M. W., "EMC Language in Perspective," 1981 IEEE EMC Symposium.

Small, J., Document (to be issued), Study of the Non-Damage Effects of Lightning on Avionics Systems, The Boeing Company.

Sommer, D. L., AFWAL-TR-81-2117, Protection of Advanced Electrical Power Systems from Atmospheric Electromagnetic Hazards, December 1981.

__________., D180-27423-17, Part 3, "Atmospheric Electricity Hazards Balanced Protection Schemes," September 1984.

Strawe, D., D180-18879-1 (AFWL-TR-75-141), Interaction of Advanced Composites With Electromagnetic Pulse (EMP) Environment, September 1975.

Tell, R. A., "Recent Results on Determining Population Exposure to VHF and UHF Broadcast Radiation in the United States," 1979 IEEE EMC Symposium.

Tenning, C. B., T6-2408, Inductive Switching Transients on the KC-135 Airplane, The Boeing Company, March 1964.

Thomas, D. E., "Measurements and Calculations of the Cross Talk Due to Capacitive Coupling Between Connector Pins," 1983 IEEE EMC Symposium.

Turner, T. E., Electrostatic Sensitivity of Various Input Protection Networks, Mostek Corp.

Vance, R. D., ITEM 1977, Magnetic Shielding.

Violette, M. F., EMC Technology, Vol. 5, Number 2, "EMI Control in the Design and Layout of Printed Circuit Boards," April 1986.

Weinstock, G. L., Electromagnetic Integration of Composite Structure in Aircraft, McDonnell Aircraft Company.

Weinstock, G. L., Intra-Vehicle Electromagnetic Compatibility Analysis, AFAL-TR--71-155, Part 1, July 1971.

White, D. R. J., "Building Attenuation and the Impact on Products Susceptibility," 1974 IEEE EMC Symposium.

__________., "EMI Control in the Design of Printed Circuit Boards," EMC Technology, January 1982.

__________., Taming EMI in Microprocessor Systems, IEEE Spectrum, December 1985.

Whittlesey, A. C., "Electric Welding Hazard to Spacecraft Electronics," 1981 IEEE EMC Symposium.

Woody, J. A., "Modeling Techniques for Discrete Passive Components to Include Parasitic Effects in EMC Analysis and Design," 1980 IEEE EMC Symposium.

Zajac, H., Study of Effects of Electrostatic Discharge on Solid State Devices, Tektronix, Inc.

Zenter, J. C., "Aircraft EMC Problems and Their Relationship to Subsystem EMI Requirements, ASD, EMC and Power Branch," WPAFB, Ohio, Proceedings IEEE, Vol. I, National Aerospace and Electronics Conference, May 17, 1983, Dayton, Ohio.

## GLOSSARY OF TERMS

ABSORPTION LOSS. Attenuation or retention of electromagnetic energy passing through a material, a shield. Absorption loss and reflection loss contribute to total shielding effectiveness (SE).

ANODIZE. A preparation by electrolytic process that deposits a protective oxide, insulating film on a metallic surface (aluminum). The oxide defeats electrical bonding. Alodine and iridite finishes on aluminum are conductive.

APERTURE. An opening, such as a nonconductive panel joint, slot or crack, allowing electromagnetic energy to pass through a shield.

AUDIO FREQUENCY (AF). The spectrum (20 to 20,000 Hz) of human hearing, often defined as extending from approximately 20 Hz to 50 kHz and sometimes to 150 kHz. Audio noise is nuisance hum, static, or tones from power line 400 Hz, switching regulator and digital clock harmonics, or HF,VHF transmitter frequencies.

BACKSHELL. Metal shell connecting circuit shields or overbraid to an electrical connector.

BALANCED CIRCUIT. A signal, acting line-to-line, between two conductors having symmetrical voltages identical and equal in relation to other circuits and to ground. "Differential mode" is line-to-line; "common mode" is line to ground.

BANDWIDTH (BW). Frequencies bounded by an upper and lower limit in a given band associated with electronic devices, filters, and receivers.

BOND, ELECTRICAL. Electrical connection at two metallic surfaces securely joined to assure good conductivity often 2.5-m maximum for electrical/electronic units and 1Ω for electrostatic dissipation or safety. A "faying surface" bond maintains contact between relatively large or long surfaces. Inherently bonded parts are permanently assembled and conductivity exists without special preparation: such as with welding, brazing.

BRAID, OVERBRAID. Fine metallic conductors woven to form a flexible conduit or cableway and installed around insulated wires to provide protection against electric fields and radio frequencies. Best when peripherally connected to backshells. A grounding strap/jumper may be made of braid.

CABLE OR HARNESS. A bundle of separate, insulated, electrical circuits, shielded or unshielded, usually long and flexible and having breakouts, terminations, overbraid, and mounting provisions completely assembled.

CABLEWAY. A solid metallic housing (liner, foil, coating) surrounding and shielding insulated electrical conductors. Also called conduit, tray, or raceway. Crosswise or transverse openings or breaks in the metallic cableway cause noise voltages to be transferred to internal wire circuits.

COMMON MODE (CM) IMPEDANCE. Impedance or resistance shared by two or more circuits so that noise voltages/currents generated by one are impressed on the others.

COMMON MODE REJECTION. The ability of wiring or an electronic device to reject common mode (line-to-ground) signals and maintain fidelity of differential mode (line-to-line) signals.

COMMON MODE SIGNAL. Identical and equal signals on input conductors or at the terminals of a device relative to ground.

CONDUCTED EMISSION (CE) OR INTERFERENCE. Voltage/current noise signals entering or leaving a unit on interface conductors-emission is the general term, interference is undesired noise.

COUPLING. The transfer of energy between wires or components of a circuit electrostatically, electromagnetically, or directly.

CROSS COUPLING (CROSSTALK). Transfer of signals from one channel, circuit, or conductor to another as an undesired or nuisance signal or the resulting noise.

DAMAGE. The irreversible failure of a component.

DECIBEL (dB). Decibel expresses the ratio between two amounts of power, P1 and P2, at two separate points in a circuit. By definition, the number of dB = 10 log to the base 10 of (P1/P2). For special cases, when a standard power level P2 = 1 mW or 1 W or 1 kW, then the ratio is defined as "dBm," "dBw," or "dBKW." Because $P = V^2/R$ and also $I^2/R$, decibels express voltage and current ratios. Ideally, the voltages and currents are measured at two points having identical impedances. By definition, dB = 20 log V1/V2 and dB = log I1/I2. For convenience, V2 or I2 are often chosen as 1 μV or 1 μA and the ratio is defined as dB above a μV or dB above a μA when graphing emission or susceptibility limits.

DIELECTRIC STRENGTH. Voltage withstand capability that an insulating material sustains before destructive arcing and current flow, usually expressed in volts per mil thickness. Dielectric withstand voltage is the voltage level at which insulation breakdown occurs.

DIFFERENTIAL MODE (DM) SIGNAL. The signal in a two-wire circuit measured from line-to-line.

DUAL GROUND. Equipment case ground/return through two independent circuit paths to structure implemented in flammable zones and water leakage areas-each path meeting electrical conductivity (resistance) requirements.

ELECTRIC FIELD. High-impedance, radiated voltage field, positive or negative, from a voltage source as contrasted to a low-impedance magnetic field from a current source.

ELECTROMAGNETIC COMPATIBILITY (EMC). Operation within performance specification in the intended electromagnetic interference environment.

ELECTROMAGNETIC INTERFERENCE (EMI). Conducted and radiated voltage/current noise signals, broadband (BB) or narrow band (NB), that degrade the specified performance of equipment.

ELECTROSTATIC CHARGE. Electric potential energy with a surrounding electric field, uniform or nonuniform, moving or at rest, on a material.

EMISSION. Voltage/current noise on a wire or in space. Broadband emission has uniform spectral energy over a wide frequency range and can be identified by the response of a measuring receiver not varying when tuned over several receiver "bandwidths." Or, energy present over a bandwidth greater than the resolution bandwidth where individual spectral components cannot be resolved. Broadband (BB) may be of two types: (1) impulse and coherent varies 20 dB per decade of bandwidth and (2) random or statistical, varies 10 dB per decade. A narrow band (NB) emission or signal, sometimes called continuous wave, occurs at a discrete frequency and does not vary with bandwidth.

FAULT CURRENT. The maximum current (magnitude and duration) flowing through a fault point-equal to the supply voltage divided by the dc resistance of power line leads, circuit breakers, and the current return in wire or structure.

FILTERING. Device or unit that passes or rejects a frequency band and designed to block noise from entering or leaving a circuit or unit.

GROUND. A generic term having multiple meanings and indicating a circuit return path or a voltage reference: not "zero" voltage reference. Four hundred millivolts of noise voltage is common on "quiet" grounds. There are several types of returns and references.

Return:

- Structure, for power, fault, and "discrete" circuits.
- A grid of wires, solid sheet, or foil.
- A wire from circuit load back to source or to case.
- Circuit card "ground plane," also a reference and shield.

Reference:

- Structure, for electronics, shields, power.
- A grid of wires, solid sheet, or foil.
- A wire from circuit to grounding block or case.
- A wire from circuit to structure.

- Shield tie.

- Earth.

IMMUNITY. Capability of a circuit or unit to operate within performance specification in a specified electromagnetic interference environment.

ISOLATION. Electrical separation and insulation of circuits from ground and other circuits or arrangement of parts to provide protection and prevention of uncontrolled electrical contact.

JUMPER/STRAP. A short wire, strip, strap, or braid conductor installed to make a safety ground connection, to dissipate electrostatic charge, or establish continuity around a break in a circuit.

LIMITING, VOLTAGE/CURRENT. Semiconductor components, diodes, Transorb, or filter designed to clip and shunt to ground an applied transient or steadystate voltage. Used to protect against noise frequencies, faults, lightning, and inductive switching transients.

MAGNETIC FIELD. A radiated, low-impedance field having lines of "flux" or magnetomotive force associated with an electrical current.

MALFUNCTION. Failure or degradation in performance that compromises flight safety.

NOISE. Conducted or radiated emission causing circuit upset, performance disorder, or undesired sound.

PRECIPITATION STATIC (P-static). Electrostatic discharge, corona, arcing, and streamering, steady state or impulsive, causing circuit upset, receiver noise or component damage.

RADIATED EMISSION (RE). Electromagnetic energy transmitted and propagated in space usually considered as audio frequency or radio frequency noise.

RADIO FREQUENCY (RF). Frequencies in the electromagnetic spectrum used for radio communications extending from kilohertz to gigahertz.

RADIO FREQUENCY INTERFERENCE (RFI). Electromagnetic interference in the radio frequency range.

SEALANT. An applied substance enclosing and protecting the integrity of a joint, fastener, or electrical bond from moisture, contaminants, oxidation, and acid or alkaline corrosion.

SHIELD. A conductive material, opaque to electromagnetic energy, for confining or repelling electromagnetic fields A structure, skin panel, case, cover, liner, foil, coating, braid, or cable-way that reduces electric and magnetic fields into or out of circuits or prevents accidental contact with hazardous voltages.

SHIELD EFFECTIVENESS (SE). The ability of a shield to reject electromagnetic fields. A measure of attenuation in field strength at a point in space caused by the insertion of a shield between the source and the point.

SIGNAL RETURN. A wire conductor between a load and the signal or driving source. Structure can be a signal and power return. Commonly, it is the low voltage side of the closed loop energy transfer circuit.

SINGLE-ENDED CIRCUIT. A circuit with source and load ends grounded to case and structure and using structure as return.

STRUCTURE. Basic members, supports, spars, stanchions, housing, skin panels, or coverings that may or may not provide conductive return paths and shields for electrical/electronic circuits.

SUSCEPTIBILITY. Upset behavior or characteristic response of an equipment when subjected to specified electromagnetic energy-identified with the point, threshold, or onset of operation outside of performance limits. Conducted Susceptibility (CS) applies to energy on interface conductors; Radiated Susceptibility (RS) to radiated fields.

THRESHOLD, NOISE. The lowest electromagnetic interference signal level that produces onset of susceptibility.

UPSET. Temporary interruption of performance that is self-correcting or reversible by manual or automatic process.

UNACCEPTABLE RESPONSE. Upset, degradation of performance, or failure, not designated a malfunction, but is detrimental or compromising to cost, schedule, comfort, or workload.

UNDESIRABLE RESPONSE. Change of performance and output, not designated a malfunction or safety hazard, that is evaluated as acceptable as is because of minimum nuisance effects and excessive cost burdens to correct.

VALIDATION. Demonstration and authentication that a final product operates in all modes and performs consistently and successfully under all actual operational and environmental conditions founded upon conformance to the applicable specifications.

VERIFICATION. Demonstration by similarity, previous in-service experience, analysis, measurement, or operation that the performance, characteristics, or parameters of equipment and parts demonstrate accuracy, show the quality of being repeatable, and meet or are acceptable under applicable specifications.

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| A/C | Aircraft |
| ACARS | ARC Communications Addressing and Reporting System |
| ACT | Active Controls Technology |
| ADC | Air Data Computer |
| AF | Audio Frequency |
| ADF | Automatic Direction Finder |
| AFCS | Automatic Flight Control System |
| ANSI | American National Standards Institute |
| APU | Auxiliary Power Unit |
| ARC | Aeronautical Radio, Inc. |
| ASDS | Airport Surface Detection System |
| ATCRBS | Air Traffic Control Radar Beacon System |
| BB | Broadband |
| BITE | Built-In Test Equipment |
| BW | Bandwidth |
| CAS | Criticality Advisory System |
| CDU | Control Display Unit |
| CE | Conducted Emission |
| CM | Common Mode |
| CRT | Cathode Ray Tube |
| CS | Conducted Susceptibility |
| DFDAU | Digital Flight Data Acquisition Unit |
| DFDR | Digital Flight Data Recorder |
| DITS | Digital Information Transfer System |
| DM | Differential Mode |
| DME | Distance Measuring Equipment |
| E | Electromagnetic Environmental Effects |
| EADI | Electronic Attitude Director Indicator |
| ECAC | Electromagnetic Compatibility Analysis Center |
| ECS | Environmental Control System |
| E/E | Electrical/Electronic |
| EEC | Electronic Engine Control |
| EED | Electro-Explosive Device |
| E-FIELD | Electric Field |
| EFIS | Electronic Flight Instrument System |
| EGT | Exhaust Gas Temperature |
| EHSI | Electronic Horizontal Situation Indicator |
| EICAS | Engine Indication and Crew Alerting System |
| EM | Electromagnetic |
| EMC | Electromagnetic Compatibility |
| EME | Electromagnetic Effects |
| EMI | Electromagnetic Interference |
| EMIC | Electromagnetic Interference/Compatibility |
| EMP | Electromagnetic Pulse |
| EPR | Engine Pressure Ratio |
| ESD | Electrostatic Discharge |

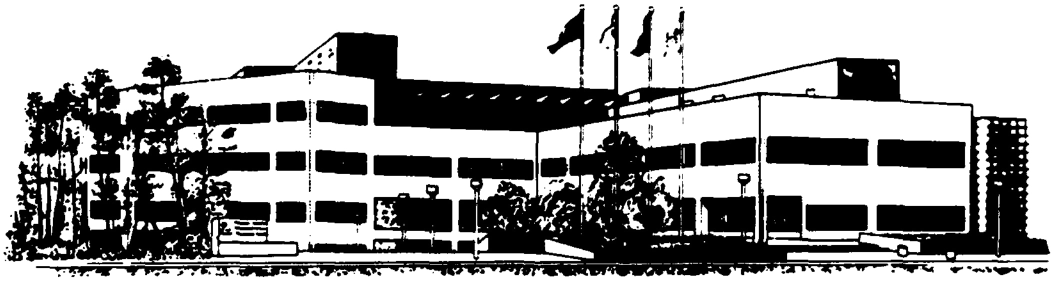
| | |
|---|---|
| ESE | Electric (field) Shield Effectiveness |
| FCC | Flight Control Computer |
| FDEP | Flight Data Entry Panel |
| FMC | Flight Management Computer |
| Gr/Ep | Graphite/Epoxy |
| GPS | Global-Positioning-System |
| GPWS | Ground Proximity Warning System |
| HF | High-Frequency |
| H-FIELD | Magnetic Field |
| IAAC | Integrated Application of Active Controls Technology (to an Advanced Subsonic Transport Project) |
| IDG | Integrated Drive Generator |
| ILS | Instrument Landing System |
| INS | Inertial Navigation System |
| IRS | Inertial Reference System |
| LCC | Life Cycle Cost |
| LOC | Localizer |
| LRRA | Low Range Radio Altimeter |
| LRU | Line Replaceable Unit |
| MCDP | Maintenance Control and Display Panel |
| MCP | Mode Control Panel |
| mil | One thousandths of an inch (0.001) |
| MLS | Microwave Landing System |
| MSE | Magnetic (Field) Shielding Effectiveness |
| NB | Narrow Band Signal |
| H1 | Fan Speed |
| N2 | Core Engine Speed |
| OMEGA | Very Low Frequency Navigation |
| PCU | Power Control Unit |
| PRF | Pulse Repetition Frequency |
| P-static | Precipitation Static |
| PWM | Pulse Width Modulation |
| RDMI | Radio Distance Magnetic Indicator |
| RE | Radiated Emission |
| RF | Radio Frequency |
| RFI | Radio Frequency Interference |
| RS | Radiated Susceptibility |
| RTCA | Radio Technical Commission for Aeronautics |
| S/A | Spectrum Analyzer |
| SE | Shielding Effectiveness |
| SHF | Super High-Frequency |
| TCAS | Traffic Alert and Collision Avoidance System |
| TLA | Thrust Lever Angle |
| TMC | Thrust Management Computer |
| TTL | Transistor-Transistor-Logic |
| UHF | Ultra High-Frequency |
| VHF | Very High-Frequency |
| VLF | Very Low-Frequency |
| VOR | VHF Omnidirectional Range |
| VORTA/VHF | Omnirange/Tactical Air Navigation |
| VSI | Vertical Speed Indicator |
| WRU | Weapons Replaceable Unit |

U.S. Department of Transportation
●deral Aviation Administration

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 12
## FAST RISE-TIME ELECTRICAL TRANSIENTS IN AIRCRAFT



**PREPARED BY:**

**COMPUTER RESOURCE MANAGEMENT, INC.**
**950 HERNDON PARKWAY, SUITE 360**
**HERNDON, VIRGINIA 22070**

**PREPARED FOR:**

**FEDERAL AVIATION ADMINISTRATION**
**TECHNICAL CENTER**
**ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405**

## NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

# 1. INTRODUCTION

## 1.1 Topic History

Fast rise-time transients have always had potentially serious effects upon aircraft structures, wiring, and systems. With the application of fly-by-wire control systems to engines and control surfaces, an understanding of the nature and effects of fast transients is now even more essential for certifi-cation authorities.

The measures, which can be taken to protect aircraft and their systems against fast transients, must also be understood for certification authorities to decide whether an aircraft is adequately protected.

Solid state devices and digital systems have improved reliability by orders of magnitude compared to the vacuum tubes, analog systems, and electromechanical devices which they replaced. Unfortunately, solid state devices and digital systems are far more susceptible to electromagnetic interference than were the older devices. Therefore, much care must be given early in the design phases of new systems to ensure against upset or damage from a wide variety of electromagnetic fields generated both by the aircraft systems themselves and by sources external to the aircraft.

This chapter describes and analyses some of the fast rise-time transients to which modern aircraft are exposed. Estimates are made of the energy levels and field strengths which these transients are capable of generating. These energy levels and field strengths are compared to the typical upset and damage thresholds which exist in aircraft systems and devices. Various methods of testing systems for susceptibility to fast transients are described. Finally, the measures which can be taken to protect systems and devices from these transients are described.

## 1.2. Topic Overview

Fast rise-time transients include the Nuclear Electromagnetic Pulse (NEMP), lightning, and Electrostatic Discharge (ESD). The primary power lines of aircraft are also subject to fast transient disturbances. These types of transients will also be described.

Historically, there has been a large difference in the levels of electromagnetic protection applied to civil and military aircraft. Civil aircraft are subject to the rather modest requirements of Radio Technical Commission for Aeronautics (RTCA) DO-160B. Military aircraft are subject to the rigorous requirements of MIL-STD-461C and MIL-STD-462.

Recently there has been widespread recognition that the electromagnetic environment is similar for many military and civil aircraft (One notable exception is the very severe environment to which Navy carrier aircraft are exposed.) Ground-based radar systems to which aircraft are exposed are much the same at military and civilian airports. Many airports are jointly used by both civil and military aircraft. Air traffic control routes and procedures expose civil and military aircraft to a similar electromagnetic environment. In the future, the Electromagnetic Compatibility (EMC) requirements for civil aircraft will be close to the requirements for military aircraft.

The potential for exposure of civil aircraft to the NEMP is a debatable point, but the civil air fleet constitutes a logistical reserve for the military. More importantly, the electrical characteristics of NEMP, lightning, and ESD are so similar that a description of all three and a comparison of their characteristics is useful as a tutorial method. Furthermore, the methods used to protect aircraft against all these transients have much in common.

In this chapter, military specifications and test methods are referenced. It is recognized that these specifications and methods do not apply directly to civil aircraft, but a thorough knowledge of the military approach is most important for understanding the evolving field of aircraft EMC.

The effects of lightning are addressed in chapter 13 of this handbook, and therefore will not be covered in depth in this chapter. The characteristics which the lightning transient has in common with other fast transients will, however, be explored.

### 1.3. Function Criticality

The fast transients described have the capability of upsetting or damaging a variety of systems which are critical to the continued safe flight and landing of the aircraft.

For junction type devices (which include transistors, integrated circuits, and diodes) it is usual to assign a burnout level of 100 microjoules. This energy level can easily be exceeded when an aircraft is subjected to NEMP, lightning, or ESD.

The consequences of circuit damage are obvious: the circuit function will be lost or at least impaired. Backup systems may have to be called into service.

Circuit upset, short of damage, may also occur. Transistor-Transistor Logic (TTL) circuits can be upset by spurious voltages of 0.4 volts. The electromagnetic fields generated within the aircraft by fast transients can generate voltages which readily exceed this value.

There are several possible consequences of circuit upset. An automatic computer controlled reset may occur. A manual reset by a flight crew member may be necessary. Or it may be necessary to completely power down a system and restart it.

The consequences of upset or damage depend, of course, on what the affected system is controlling and how long it takes to reset the system or bring backup controls into operation. Obviously, loss of engine or flight surface controls may be extremely critical depending upon the phase of flight. Loss of navigation or communications systems is less critical. The presence of backup systems, such as on present day fly-by-wire engine controls, greatly affects the criticality.

## 2. TRANSIENT ANALYSIS: THE DOUBLE EXPONENTIAL PULSE

Lightning, NEMP, and ESD can all be described in terms of the double exponential pulse. The common characteristics of all three phenomena are that they display a fast rise-time followed by a much slower fall-time. Such a pulse is shown in figure 2-1.

For each type of pulse, the rise- and fall-times are different, and the maximum voltages or currents are different, but the pulse shapes are similar.

The NEMP has a rise-time of about 5 nanoseconds and a fall-time of perhaps 600 nanoseconds. Lightning has traditionally been assigned a rise-time of 1 to 2 microseconds and a fall-time of 50 to 100 microseconds. However, recent investigations have shown that a significant proportion of lightning discharges have rise-times in the range of 200 nanoseconds or less. The ESD pulse has a typical rise-time (10 percent to 90 percent) of 2 nanoseconds, and a fall-time to the 50 percent level of 200 nanoseconds.

The ESD pulse has an amplitude of from 1 to 30 kilovolts. The NEMP pulse has an amplitude of about 50 kilovolts, and the voltage induced by lightning on an aircraft structure can range up to about 60 kilovolts, although the peak voltage of the lightning strike itself may be much higher. The voltages induced on aircraft wiring by lightning and NEMP are much smaller, on the order of 600 to 1500 volts, and voltages of this magnitude are often specified in pin level tests of system cabling.

Mathematically, the voltage of the double exponential pulse can be represented as:

$$V = V_0 \left(e^{-at} - e^{-bt}\right) \tag{1}$$

where the fast rise is governed by the "b" coefficient, and the slow fall is governed by the "a" coefficient.

The fast transient pulse itself can be compared to a hammer blow. The response of the aircraft structure, cabling, and systems can be compared to the ringing of a bell when struck by the hammer.

### 2.1. A Distinction between Lightning, NEMP, and ESD

The following analysis applies principally to the NEMP and to the indirect effects of lightning. Because the source impedance of an electrostatic discharge is a function of frequency and is also much higher than that of NEMP and lightning, the system response to ESD is somewhat different, and its analysis will be addressed separately.

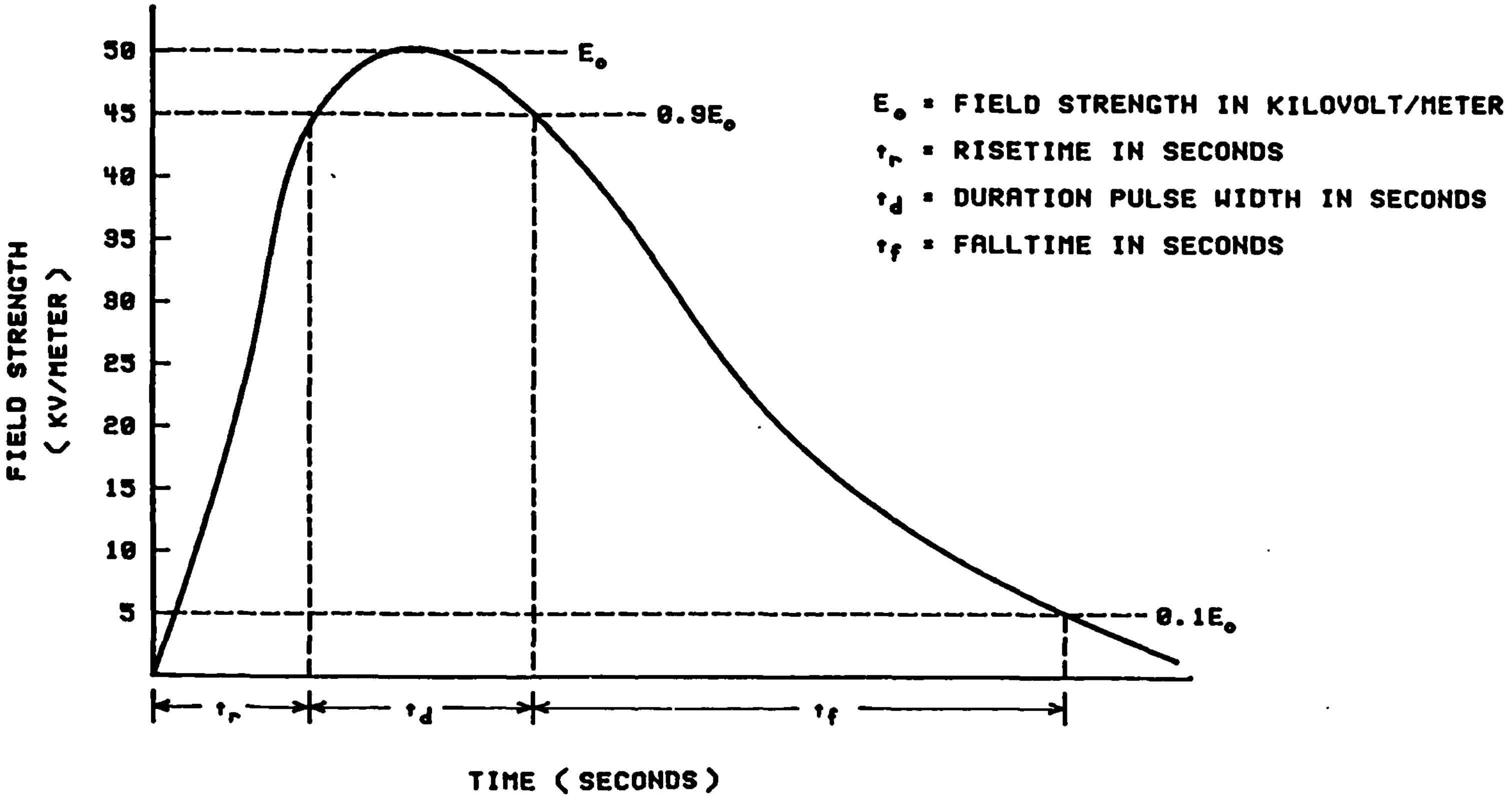


FIGURE 2-1. DOUBLE EXPONENTIAL PULSE

## 2.2. Response of the Aircraft to Lightning and NEMP

The size of the aircraft, the length of the cables within it, and the exact method of electrical termination of those cables determine the response of the aircraft to the double exponential pulse.

For example, in a large commercial transport, if a long cable in the wings or fuselage is terminated at one end with a low impedance, and at the other end in a high impedance, the cable can resonate in a quarter wavelength mode. The resulting resonant frequency might be on the order of 1 Megahertz (MHz).

When the double exponential pulse excites a resonant system in the aircraft, the response is an exponentially damped sinusoidal wave form. The frequency of this sinusoidal response is determined by the dimensions of the structure or cabling. The damping is determined by the energy storage and losses of the aircraft system, or quality factor, Q.

The resulting waveform can be represented mathematically as:

$$V = V_0 \left(e^{-at} - e^{-bt}\right) \cos(2\pi f_0 t) \tag{2}$$

where $f_0$ is the resonant frequency assigned to the aircraft structure or cabling. The rise- and fall-times are not those of the excitation pulse, but are determined by the physical properties of the resonant system. "Physical properties of the resonant system" refer to the energy storage capabilities of the aircraft wiring (determined by the inductance and capacitance of the wiring) and to the resistive losses (determined by the loads connected to the cables).

The voltage $V_0$ in Equation 2 is a function of the exciting pulse amplitude, the aircraft fuselage shielding, and the cable shielding. $V_0$ is usually much smaller than the voltage amplitude of the double exponential pulse itself.

A simpler version of Equation 2 is often used to represent the aircraft system response:

$$V = 1.05\ V_0 \left(e^{-at}\right) \sin(2\pi f_0 t) \tag{3}$$

In this representation the rise-time is governed by the choice of the system resonant frequency. The rise-time is on the order of the time required for the sine wave to rise from zero to its first peak, at one-quarter of one period of the resonant frequency. The "a" coefficient, which determines the rate of decay, is defined as $\pi\ f_0/Q$. The value of Q is usually between 15 and 25 for aircraft cabling systems.

This form of the equation is somewhat more easily analyzed than that of Equation 2 and will be used throughout this chapter. Although Equation 2 is a more exact representation than is Equation 3, the differences between them in terms of maximum voltage, maximum current, frequency spectrum, and energy transfer are negligible.

It should be noted that the $V_o$ and "a" terms in Equation 1 and Equation 3 are not the same. The only connection is that the peak amplitude of the system response is proportional to the peak amplitude of the NEMP or lightning pulse.

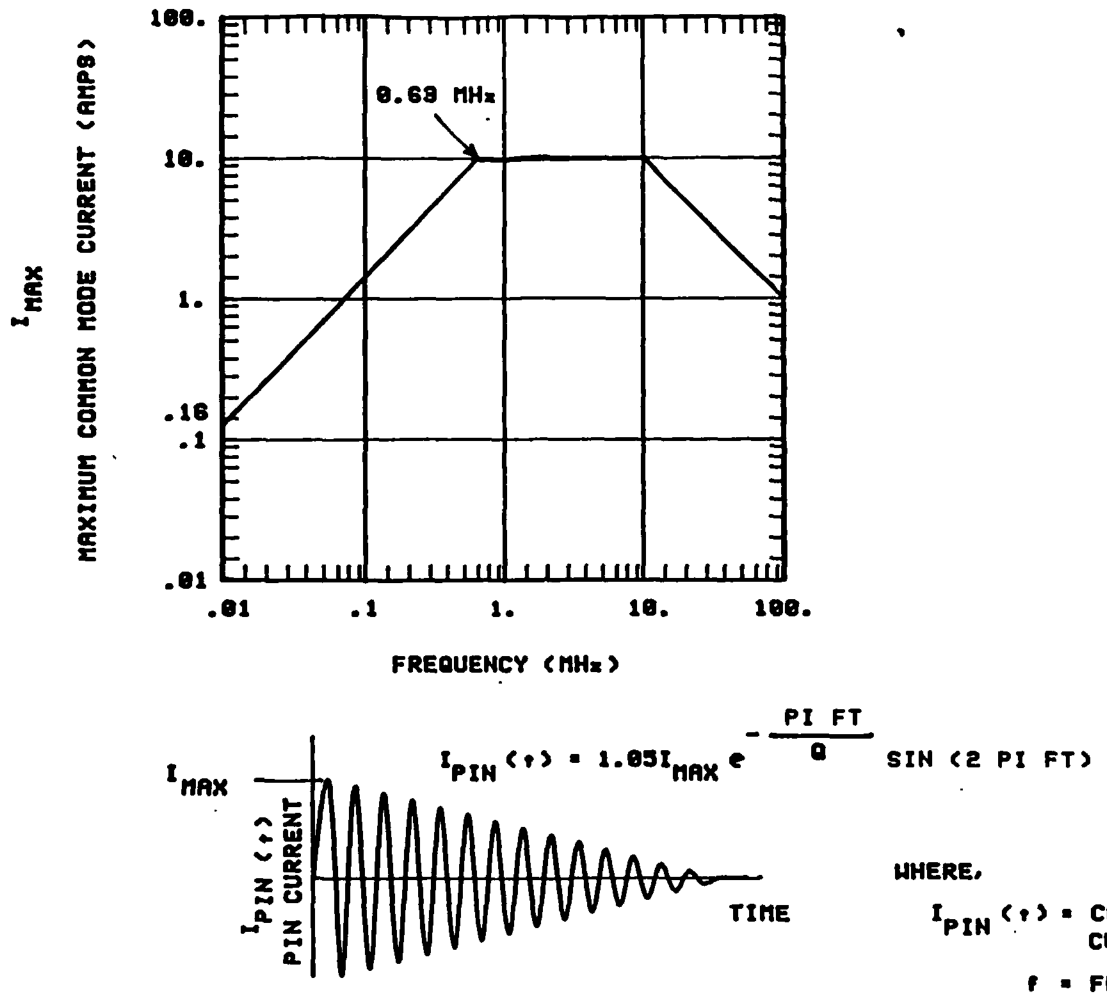
In Equation 3 the coefficient 1.05 is a function of the Q of the system, and can vary from about 1.03 to 1.05 as the Q varies from 15 to 25 in typical resonant structures. The exact value of this coefficient is:

$$k = e^{\frac{\pi}{4Q}} \tag{4}$$

This coefficient, multiplied by the maximum voltage induced on the cabling ($V_o$), yields an initial over-voltage such that when the falling exponential curve meets the rising sinusoidal curve, the resulting voltage is the maximum voltage of the transient response. The exact value of k is not particularly critical to the energy analysis, but the value assigned to Q is, since the energy of the system response is closely proportional to Q.

For NEMP analysis, the voltage $V_o$ is replaced with a current $I_o$. MIL-STD-461 CS10 and CS11 define $I_o$ as in figure 2.2-1. The current shown in figure 2.2-1 represents the current that could be induced on aircraft wiring when the aircraft is subjected to a NEMP or a NEMP simulator during testing. Figure 2.2-1 also shows the exponentially *damped sinusoidal waveform*.

Lightning and NEMP test requirements may specify either the voltage or the current of the test waveform. Through a knowledge of system impedances and with the use of Ohm's Law, voltages and currents can be rendered equivalent to one another.



$$I_{PIN}(t) = 1.05 I_{MAX}\, e^{-\frac{PI\ FT}{Q}} \; SIN\ (2\ PI\ FT)$$

WHERE,

$I_{PIN}$ (t) = COMMON MODE PIN CURRENT IN AMPS

f = FREQUENCY, HERTZ

t = TIME, SECONDS

Q = DECAY FACTOR

FIGURE 2.2-1. NEMP CURRENT

## 3. ENERGY TRANSFER FROM THE PULSE TO THE SYSTEM

When the double exponential pulse is applied to the system, and the system responds in its resonant fashion, energy is transferred from the pulse into the system. It is this energy which can cause upset or damage.

In a pin-level test the voltage of Equation 3 is applied directly to one of the conductors in a multiconductor cable. If the source resistance of the testing device and the load resistances connected to each end of the cable are known, the power developed in the system is then found by squaring Equation 3 and dividing the result by the sum of the source and load resistances.

The total power is:

$$P = \frac{V^2}{(R_S + R_L)} \qquad (5)$$

where V is obtained from Equation 3. $R_S$ is the source resistance of the testing device and $R_L$ is the load resistance of the cable under test.

To find the energy in the system, it is necessary to integrate Equation 5 with respect to time. The total energy delivered to both source and load is:

$$E_t = \frac{k^2 V_0^{\ 2}}{(R_S + R_L)} \int_0^{\infty} e^{-2at} \sin^2(w_0 t) dt \qquad (6)$$

The total energy is divided between the source and load resistances as follows:

$$E_S = \frac{E_t R_S}{(R_S + R_L)} \qquad (7)$$

$$E_L = \frac{E_t R_L}{(R_S + R_L)} \qquad (8)$$

where $E_S$ and $E_L$ are the energy into the source and load resistances, respectively.

Integrating Equation 6 and allocating the energy to source and load as in Equations 7 and 8 produces the following equations:

$$E_S = \frac{k^2 V_o^2 R_S Q}{(R_S + R_L)^2 \left(1 + \frac{1}{4Q^2}\right)(4\pi f_o)} \quad (9)$$

$$E_L = \frac{k^2 V_o^2 R_L Q}{(R_S + R_L)^2 \left(1 + \frac{1}{4Q^2}\right)(4\pi f_o)} \quad (10)$$

### 3.1. An Energy Transfer Example

As an example of the energy that can be transferred from a NEMP or from the indirect effects of lightning, Equations 9 and 10 can be solved by assigning typical values to the variables:

$V_o$ = 600 volts<br>
$Q$ = 20<br>
$k$ = 1.04<br>
$R_S$ = 20 ohms<br>
$R_L$ = 20 ohms<br>
$f_o$ = 1 MHz

The voltage (600 volts) is typical of the voltage induced on aircraft wiring by fast transients.

The Q value of 20 is representative of aircraft systems. The source and load impedances can have many values. The values chosen are low and will result in high energy transfer.

The resonant frequency of 1 MHz is suggestive of a very large aircraft. It also implies a large energy transfer.

When Equations 9 and 10 are solved using the assigned values, 7.74 millijoules of energy are delivered to the source and to the load. The burnout level for solid state devices is often taken to be 100 microjoules, where 1 joule is equal to 1 watt-second. The calculated value of energy is 77.4 times the burnout level, so obviously there is a problem. The system affected by the transient pulse must be protected in some way.

The energy distribution of the system response in the frequency domain will now be examined. This approach will lead immediately to a low-pass filter specification which will limit the amount of transferred energy to below the burnout level.

## 4. FREQUENCY SPECTRUM OF THE SYSTEM RESPONSE

The transient response of the system as a function of time has been depicted, as shown in the lower part of figure 2.2-1. There is also a frequency spectrum representation from which the energy distribution as a function of frequency may be found.

Mathematically, the Fourier transform is used to derive the voltage as a function of frequency from its time domain representation. An explanation of the Fourier transform is beyond the scope of this chapter. However, the frequency spectrum derived through the Fourier transform is shown in figure 4-1. The spectrum is that of a system having a resonance at 1 MHz and a Q of 20. The amplitude scale at the left is in decibels (dB), with the zero dB level corresponding to the voltage in the system at zero frequency. The voltage at resonance is Q times the voltage at zero frequency. From this consideration it may be observed that the voltage peak at resonance is 20 Log Q dB above the zero frequency reference level. The bandwidth between the points 3 dB below the peak response also yields the value of Q through the relation:

$$Q = \frac{f_o}{\text{BandWidth(3dB)}} \tag{11}$$

At about two times the resonant frequency the slope of the voltage characteristic begins to approach a 40 dB per decade slope. As a consequence, the energy contribution at frequencies more than about 4 times higher than the resonance is negligible.

If the voltage versus frequency characteristic of figure 4-1 is squared, divided by the sum of the source and load resistances, and integrated with respect to frequency, the energy as a function of frequency can be found. If the integration limits are zero and infinity, the total energy over the entire frequency spectrum is found and is the same as that previously determined in the time domain by Equations 9 and 10. If the integration limits are zero and 500 kilohertz (kHz), for example, then the energy between those limits can be determined.

A program in Electromagnetic Computer aided design (EMCad$^{tm}$) usable on IBM compatible PCs has been written to perform this integration and has generated some useful guidelines for the energy distribution:

- One-half of the energy lies between the half-power (3 dB) points of the resonance.

- Approximately one-fourth of the energy lies below the lower half-power (3 dB) point of the resonance.

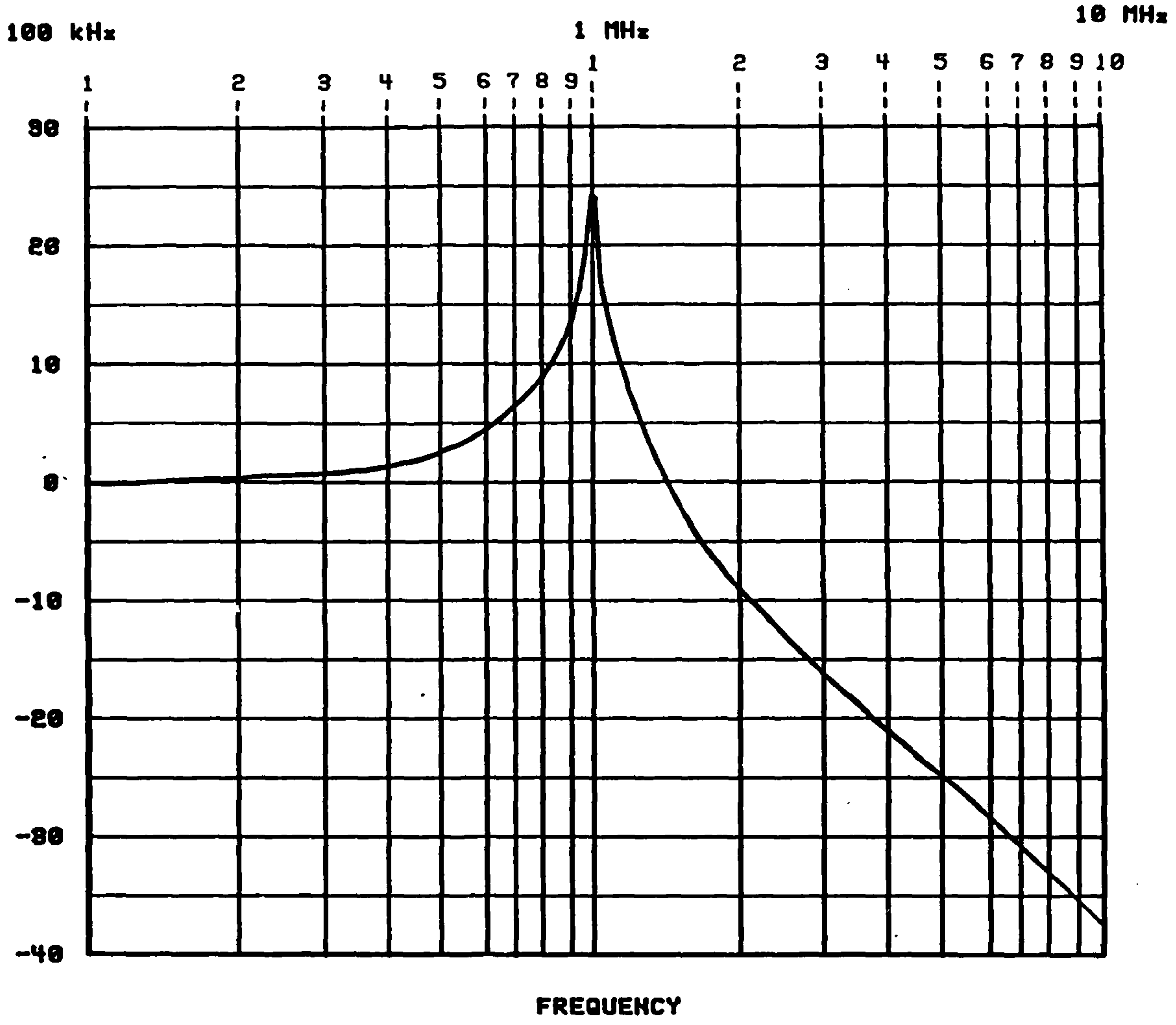


FIGURE 4-1. FREQUENCY SPECTRUM OF A 1 MHz DAMPED SINUSOID

- Approximately one-fourth of the energy lies above the upper half-power (3 dB) point of the resonance.

- Approximately 2 percent of the energy lies below 10 half-power bandwidths below the resonant frequency.

Using these guidelines, or (for more precision) the EMCad$^{tm}$ program, the frequency at which the burnout level is reached can be determined. From the examples in Equations 9 and 10, the energy delivered to the load is 7.74 millijoules. The half-power bandwidth of the 1 MHz resonance is 50 kHz (from Equation 11). The 10 half-power bandwidths below resonance then yield a frequency of 500 kHz, at which 2 percent of 7.74 millijoules will have accumulated. That is, over the frequency range from Direct Current (DC) to 500 kHz, the transient pulse will deliver 155 microjoules into the load impedance. For a more precise answer, the computer program shows that 100 microjoules will be delivered between DC and 368 kHz.

An approximate, though accurate, formula has been developed for the energy as a function of frequency. By setting the frequency equal to zero in the Fourier transform, the voltage at zero frequency can be found:

$$V(0) = \frac{V_0\ k}{2\pi f_0 \left(1 + \frac{1}{4Q^2}\right)} \tag{12}$$

Assuming that the system losses (represented by the "a" in $e^{-at}$ of Equation 6) are zero, then Q is infinite. For infinite Q, the voltage as a function of frequency is given by:

$$V = \frac{V(0)\ f_0^2}{\left(f_0^2 - f^2\right)} \tag{13}$$

This expression is extremely accurate for Q's as low as 15 up to frequencies within a few half-power bandwidths of the resonant frequency.

The total energy as a function of frequency is given by:

$$E_t = \frac{2\ V(0)^2\ f_0^4}{(R_S + R_L)} \int_0^{f_1} \frac{df}{\left(f_0^2 - f^2\right)^2} \tag{14}$$

The factor of 2 is required because the energy integral should be evaluated between limits of $-f_1$ and $+f_1$ rather than 0 and $f_1$. The integral of the time function, Equation 6, is still integrated starting from time (t) = 0 and is always zero for time before t = 0.

After integrating the expression above, the energy as a function of frequency is given by:

$$E(f) = \frac{V(0)^2 f_0^2}{(R_S + R_L)} \left[ \frac{f_1}{(f_0^2 - f_1^2)} + \frac{1}{2f_0} \mathrm{Log}_e \frac{f_0 + f_1}{f_0 - f_1} \right] \qquad (15)$$

The energy calculated here divides resistively between source and load as shown in Equations 7 and 8.

If Equation 15 is evaluated at $f_1$ and $f_2$ instead of 0 and $f_1$, the energy in any specified portion of the spectrum can be found.

Criteria for a filter design are now established. To protect the circuit with the values given earlier from energy levels above 100 microjoules, the circuit must have low-pass filtering which cuts off all energy above 368 kHz.

A NEMP or lightning specification sometimes identifies several frequencies of resonance in an aircraft, such as 1, 5, 10, and 45 MHz. Each frequency corresponds to some structural or cable dimension which resonates at a wavelength usually related to that dimension in a quarter or half-wave mode. An aircraft typically displays a multitude of resonances in the 1 to 50 MHz range.

Computer analysis has shown that if the aircraft resonances are separated in frequency by just a few half-power bandwidths, each resonance and its energy contribution may be treated as independent. A separate analysis may be made for each resonant frequency, and the energy levels from each may be added to find the total energy transfer. In a multiple-resonant system the energy contribution of each resonance scales inversely with frequency, so in many cases only the two lowest resonances make a significant energy contribution.

Multiple resonances can readily occur if a cable is resonant at 1 MHz in a quarter wave-length mode. The cable will then also be resonant at odd multiples of 1 MHz, such as 3, 5, and 7 MHz. In the numerical example worked above, if a 3 MHz resonance is assumed in addition to the 1 MHz resonance, the total energy will increase from 7.74 millijoules to 10.33 millijoules. Resonances at even higher frequencies will make only a small additional energy contribution. The voltage spectrum of a system with resonances at 1 and 3 MHz is shown in figure 4-2.

A low-pass filter, which takes care of limiting the energy transfer at the lowest frequency resonances, will also eliminate the energy transfer at the higher frequency resonances, if the filter retains its attenuation characteristics at the higher frequencies. For this reason the choice of filters or filter components, which have good high frequency characteristics, is important.

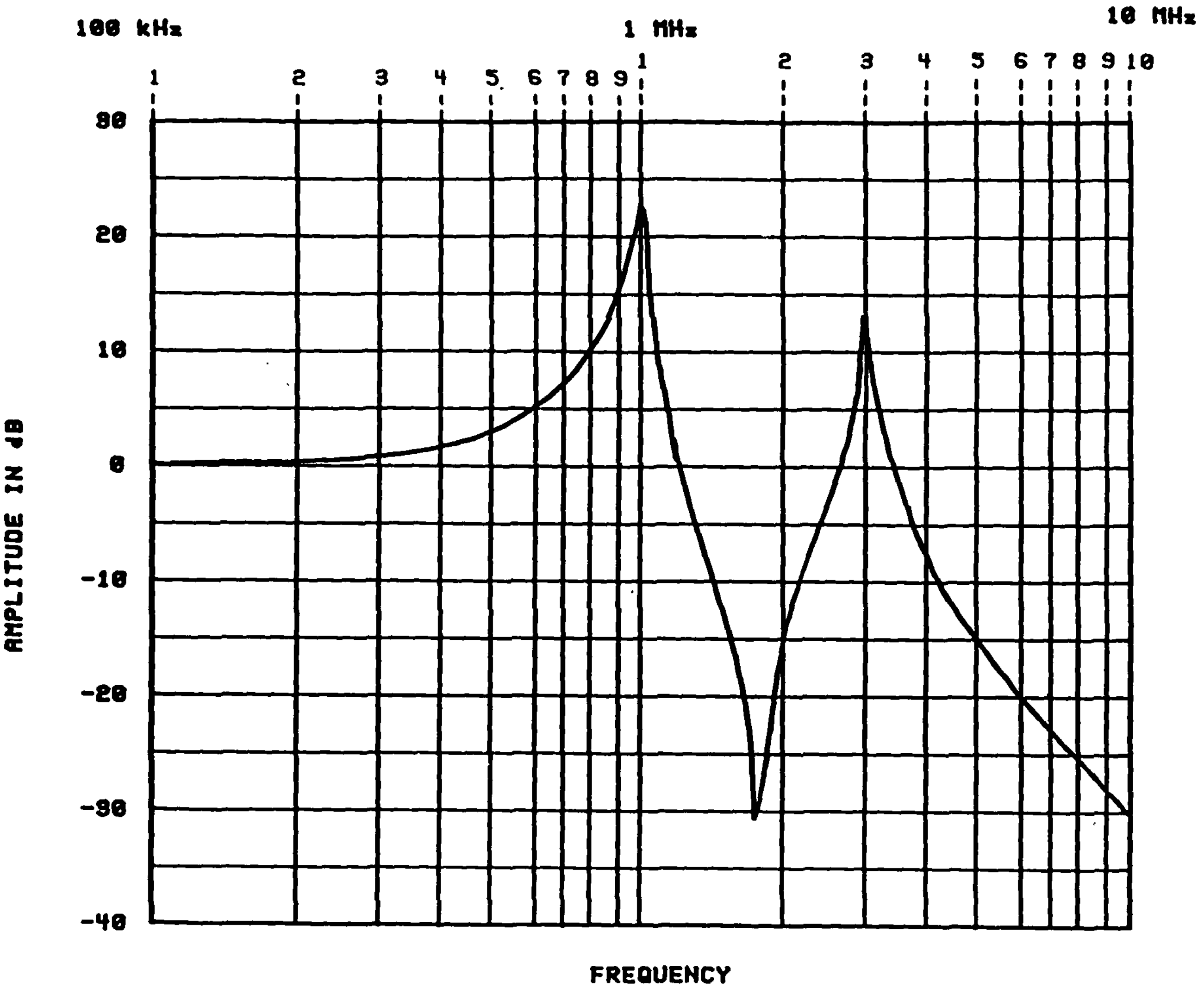


FIGURE 4-2. FREQUENCY SPECTRUM OF A DAMPED SINUSOID WITH TWO RESONANCES

If a lightning or NEMP requirement specifies only one resonant frequency, good practice dictates that a safety factor of 2 should be applied to the cut-off frequency determined by the energy analysis to eliminate the multiple resonance condition.

Since hundreds or thousands of individual circuits may have to be analyzed, a computerized approach to an evaluation of the system is essential. Spread sheets identifying conductors, load resistances, and energy levels are useful in this type of analysis. Computerized filter design programs are also helpful. The usual filter is a low-pass type, and usually only a series inductance and a shunt capacitance are required. Sometimes the necessary characteristics can be provided by a filter pin connector, in which the filter elements are incorporated into the body of the connector.

# 5. ELECTROSTATIC DISCHARGE

ESD is the familiar phenomenon experienced in stroking the back of a cat or touching a metal door knob after crossing a carpeted room. Some typical methods of generating electrostatic voltages are shown in table 5-1.

The accumulation of charge on the human body, or upon objects, can generate voltages up to 30 kilovolts. When the accumulated charge is eventually redistributed via a discharge arc, the fast rise-time pulse that results can have adverse effects on susceptible electronics equipment, ranging from upset to damage.

Aircraft are well suited for the generation of ESD. Relative humidity is often low, so that accumulated charge cannot slowly and harmlessly leak off without an arc. The decrease of atmospheric pressure with altitude somewhat decreases the insulating properties of air, and the motion of the aircraft through the air can cause an accumulation of charge. Finally, the movements of passengers and crew can cause charge accumulation in the same way as on the ground. Discharges from passengers or crew to metallic objects in the cabin can generate a field which may couple to cables routed behind decorative panels.

## 5.1. Energy Transfer in ESD

Although the waveform of the transient pulse for ESD is similar in shape to that of lightning and NEMP, the frequency spectrum of the energy transferred to the victim circuit from an ESD pulse is rather different. The source impedance of lightning and NEMP test devices, and the source impedance of the physical phenomena are usually quite low and mainly resistive. The ESD source, as shown in table 5-1, is characterized as a resistance in series with a capacitance. The impedance of this source is quite high at low frequencies and decreases with increasing frequency as the impedance of the capacitor decreases. As a result, the spectral content of an ESD has less energy at low frequencies and more at high frequencies than lightning and NEMP. Also, much higher voltages are required in ESD to generate the same total energy as for lightning and NEMP. However, the voltages available from ESD generating mechanisms are in fact very high, and the total transferred energy can be comparable to that of lightning and NEMP.

The energy of an ESD pulse may be delivered directly to a sensitive conductor or component, but more often the discharge is from the human body to a grounded object. Most of the energy is dissipated harmlessly to ground, but the flow of current to ground generates an electric field. In the analysis of ESD effects, it is useful to consider the effect of this electric field on surrounding objects in addition to the energy transfer considerations.

TABLE 5-1. TYPICAL ELECTROSTATIC VOLTAGES

| Means of Static Generation | Electrostatic Voltages | |
|---|---|---|
| | 10 to 20 Percent Relative Humidity | 65 to 90 Percent Relative Humidity |
| Walking across carpet | 35,000 | 1,500 |
| Walking over vinyl floor | 12,000 | 250 |
| Worker at bench | 6,000 | 100 |
| Vinyl envelopes for work instructions | 7,000 | 600 |
| Common poly bag picked up from bench | 20,000 | 1,200 |
| Work chair padded with polyurethane foam | 18,000 | 1,500 |

## 5.2. Description of the ESD Pulse

The typical ESD pulse is a double exponential and has been described earlier in this chapter. For easier analysis the pulse can be approximated by a triangular wave form as shown in figure 5.2-1. The frequency domain characterization of the pulse is also shown in figure 5.2-1. Significant amounts of energy appear well into the VHF region. The ESD pulse is inherently broadband, and susceptible equipment must be protected against it from very low frequencies to several hundred MHz.

This broadband pulse is capable of exciting resonances in nearby structures. The resulting response is a damped sinusoid, as shown earlier in figure 2.2-1.

## 5.3. Direct Discharge ESD

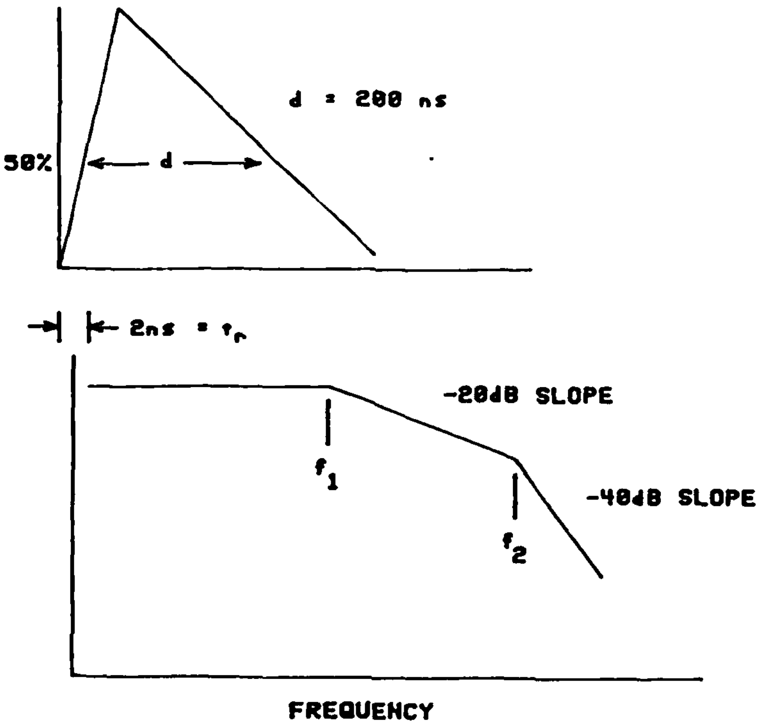
An arc from the hand to a susceptible device is called direct discharge. The human body, for ESD purposes, can be modeled as a simple series RC circuit (shown in figure 5.3-1).

For the simulation of an ESD, an ESD simulator is used (shown in figure 5.3-2). The energy stored in the human body or in the capacitor of the ESD simulator is given by 1/2 $CV^2$, where C is the capacitance and V is the voltage. This energy is in joules or watt-seconds. For a 100 pf capacitor charged to 12 kV, the total energy delivered to the series resistor and the device under test is 7.2 millijoules. The total energy divides between the series resistance and the resistance of the test device. The energy delivered to the test device can be compared to its energy specification, if given, to see if there is danger of damage. The energy division occurs as shown in Equations 7 and 8.

The time required for the voltage to decay to 1/e (37 percent) of its initial value is given by t = RC. For a series resistance of 1500 ohms and a 100 pf capacitor, t is 0.15 microseconds.

In many cases upset rather than damage is the result of this kind of discharge. This condition is best checked during actual operation of the system under test. Repeated discharges will sometimes cause upset when a single discharge does not. A single discharge may occur in the time between data bit transmissions, whereas a repeated discharge has a good chance of occurring at the time of a data bit transmission and can cause a loss or alteration of data.

Many solid state devices are very susceptible to permanent damage from ESD incidental to handling. Careful training of installation and maintenance personnel, and adherence to handling procedures is required to avoid damage. Complimentary Metal-Oxide Semiconducter (CMOS) integrated circuits are known to be particularly subject to damage by mishandling, both as isolated components and when installed on circuit boards. For the proper handling procedures for ESD sensitive components, much useful information can be obtained from ESD Control in the Manufacturing Environment, published by the Department of Defense (DOD) Reliability Analysis Center. Military Handbook DOD-HDBK-263, Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies and Equipment is also of use.



$$f_2 = \frac{1}{PI\ t_r}$$

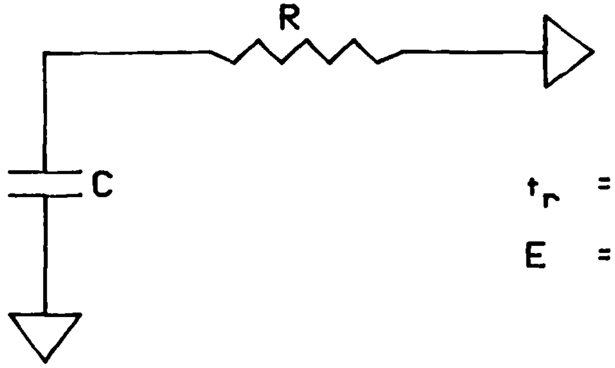
$$f_1 = \frac{1}{PI\ (\ d + t_r\ )}$$

$$C_n = \frac{2\ A\ (d + t_r\ )}{T}$$

LET $f_o$ = 1 SEC. T = 1
A = 12KV

| FREQUENCY | Cn mV | Cn dBuV | Cn dBuV/MHz |
|---|---|---|---|
| 1 Hz | 4.8 | 73.7 | 193.7 |
| $f_1$ = 1.58MHz | 4.8 | 73.7 | 193.7 |
| $f_2$ = 159MHz | 4.8 | 33.7 | 153.7 |

FIGURE 5.2-1. ESD VOLTAGE PREDICTION

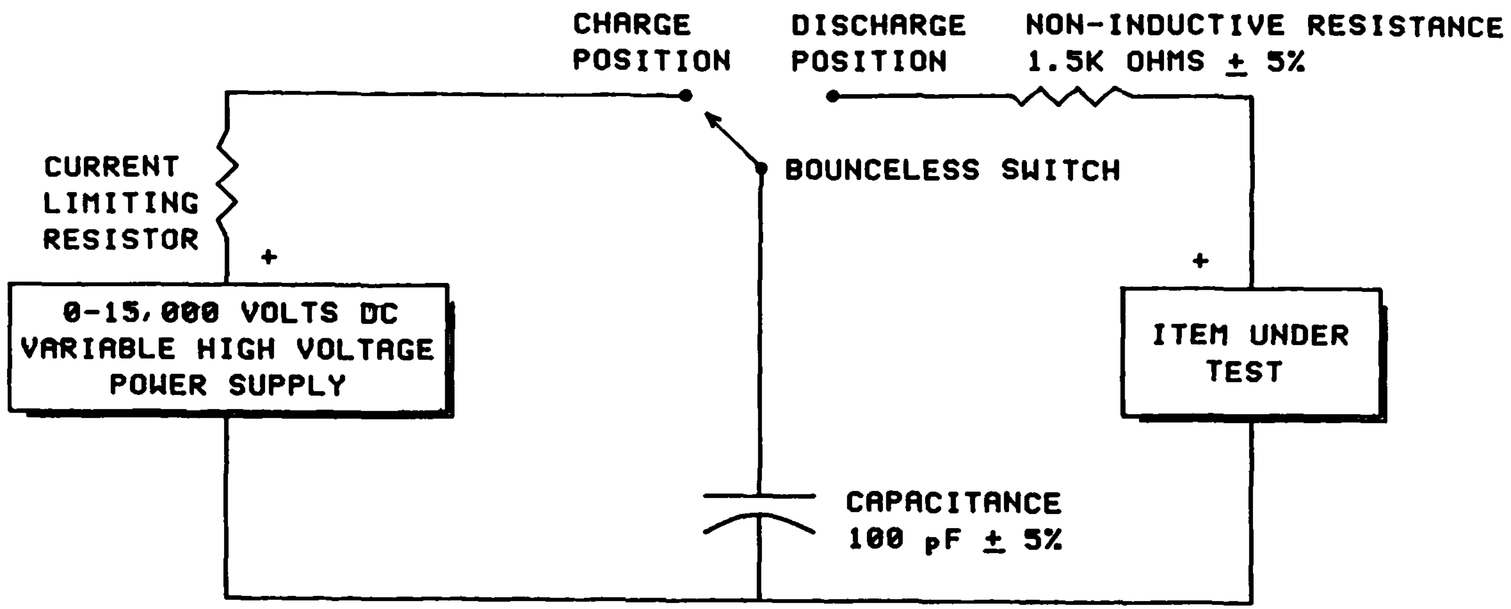


$t_r = RC$

$E = 1/2\ CV^2$

| PARAMETER | LOW | HIGH | TYPICAL |
|---|---|---|---|
| R | 5 | 100 K OHMS | 1-4 K OHMS |
| C | 25pf | .003 uf | 100-150pf |
| V | 1 kv | 30 kv | 8-12 kv |
| $t_r$ | 125 P SEC | 300 U SEC | 1-6 N SEC |
| E | 100 uJ | 1.3 J | 3-10 mJ |

FIGURE 5.3-1. HUMAN ESD MODELING


CHARGE POSITION
DISCHARGE POSITION
NON-INDUCTIVE RESISTANCE 1.5K OHMS ± 5%
CURRENT LIMITING RESISTOR
BOUNCELESS SWITCH
+
0-15,000 VOLTS DC VARIABLE HIGH VOLTAGE POWER SUPPLY
+
ITEM UNDER TEST
CAPACITANCE 100 pF ± 5%

NOTE: TEST VOLTAGES ARE MEASURED ACROSS THE CAPACITANCE. THE CAPACITOR SHALL BE DISCHARGED THROUGH THE SERIES RESISTOR INTO THE ITEM UNDER TEST BY MAINTAINING THE BOUNCELESS SWITCH TO THE DISCHARGE POSITION FOR A TIME NO SHORTER THAN REQUIRED TO DECAY THE CAPACITOR VOLTAGE TO LESS THAN 1 PERCENT OF THE TEST VOLTAGE OR 5 SECONDS, WHICHEVER IS LESS. POWER SUPPLY VOLTAGE SHALL BE WITHIN A TOLERANCE OF ± 5 PERCENT OF TEST VOLTAGE.

*FIGURE 5.3-2. ESD TEST CIRCUIT*

Table 5.3-1 lists a wide variety of electronic devices, grouped by their sensitivity to the voltage of an ESD. Table 5.3-2 shows the failure mechanisms that occur in various devices from ESD exposure.

Testing for direct discharge effects is performed as shown in figure 5.3-3. In the laboratory, the Alternating Current (AC) power would be provided as shown. On board an aircraft, it may be convenient to power the ESD simulator from batteries. Systems are best checked by operating them and watching for upset or damage when the ESD pulse is applied.

The effects of ESD on a digital system can range from missing data, to a condition requiring reset of the system, to damage requiring the replacement of parts.

## 5.4. Prediction of ESD Radiated Electric Fields

In the following example, a prediction is made of the effects of an ESD from the human hand to a metallic object in the cockpit of a commercial transport. A cabin attendant comes forward, touches a metallic object located one meter away from a susceptible item of equipment, and causes a discharge to occur. This analysis starts with the triangular pulse approximation of figure 5.2-1, and uses the chart in table 5.4-1 to guide the calculations.

In table 5.4-1, the amplitude of the pulse is 12 kV, which is quite typical of the ESD associated with the human body. The Fourier coefficient, which gives the amplitude of the pulse in the frequency domain, is $C_n$ measured in dB microvolts per MHz. Note in the legend at the bottom of figure 5.2-1 that the amplitude as a function of frequency is constant from essentially DC to 1.58 MHz and then decreases at a rate of 20 dB per decade to 159 MHz. Above 159 MHz the amplitude decreases at a rate of 40 dB per decade. The electric field strength that is generated at a distance of one meter from this 12 kV discharge can now be calculated.

Referring to the frequency column of table 5.4-1, 1.58 MHz was entered as the frequency at which the radiated field of a 12 kV discharge was first calculated. Enter in column 1, 193.7 dBμV/MHz, the Fourier coefficient obtained in figure 5.2-1. In column 2 enter -34 dB, which is a standard transfer function value to convert from a voltage on a conductor to the electric field generated one meter away. In column 3 enter a figure in dB (for the antenna factor) to determine how efficient the source is as a radiator of energy. This calculation compares the level of radiation from a short antenna to that of a quarter wave-length antenna at the same frequency. In this case, the entire human body is the major part of the radiating circuit and can be determined to be 2 meters. Using Note 3 in table 5.4-1, the antenna factor is calculated as 13.8 dB. Finally, in columns 4, 5, and 6 enter dB values for the number of conductors carrying the signal for the distance from the discharge to the susceptible nearby equipment and for the height above ground of the radiating object. Values of zero dB have been entered in each of these columns, indicating one conductor, a distance of 1 meter, and a height above ground of 0.5 meters.

TABLE 5.3-1. ESD PARTS BY PART TYPE

**CLASS 1: SENSITIVITY RANGE 0 TO $\leq$ 1000VOLTS**

- Metal Oxide Semiconductor (MOS) devices including C, D, N, P, V, and other MOS technology without protective circuitry, or protective circuitry having Class 1 sensitivity
- Surface Acoustic Wave (SAW) devices
- Operational Amplifiers (OP AMP) with unprotected MOS capacitors
- Junction Field Effect Transistors (JFETs) (Ref.: Similarity to MIL-STD-701: Junction field effect transistors and junction field effect transistors, dual unitized)
- Silicon Controlled Rectifiers (SCRs) with Io $< 0.175$ amperes at 100° Celsius (° C) ambient temperature (Ref.: Similarity to MIL-STD-701: Thyristors (silicon controlled rectifiers))
- Precision Voltage Regulator Microcircuits: Line or Load Voltage Regulation $< 0.5$ percent
- Microwave and Ultra-High Frequency Semiconductors and Microcircuits: Frequency $> 1$ gigahertz
- Thin Film Resistors (Type RN) with tolerance of $\leq 0.1$ percent; power $> 0.05$ watt
- Thin Film Resistors (Type RN) with tolerance of $> 0.1$ percent; power $\leq 0.05$ watt
- Large Scale Integrated (LSI) Microcircuits including microprocessors and memories without protective circuitry, or protective circuitry having Class 1 sensitivity (Note: LSI devices usually have two or three layers of circuitry with metallization crossovers and small geometry active elements)
- Hybrids Utilizing Class 1 parts

TABLE 5.3-1. ESD PARTS BY PART TYPE (Continued)

| CLASS 2: SENSITIVITY RANGE $>1000$ TO $\leq 4000$ VOLTS |
|---|
| • MOS devices or devices containing MOS constituents including C, D, N, P, V, or other MOS technology with protective circuitry having Class 2 sensitivity<br>• Schottky diodes (Ref.: Similarity to MIL-STD-701: Silicon switching diodes (listed in order of increasing tr))<br>• Precision Resistor Networks (Type RZ)<br>• High Speed Emitter Coupled Logic (ECL) Microcircuits with propagation delay $\leq 1$ nanosecond<br>• Transistor-Transistor Logic (TTL) Microcircuits (Schottky, low power, high speed, and standard)<br>• Operational Amplifiers (OP AMP) with MOS capacitors with protective circuitry having Class 2 sensitivity<br>• LSI with input protection having Class 2 sensitivity<br>• Hybrids utilizing Class 2 parts |

TABLE 5.3-1. ESD PARTS BY PART TYPE (Continued)

| CLASS 3: SENSITIVITY RANGE $>$4000 TO $\leq$15,000 VOLTS |
|---|
| • Lower Power Chopper Resistors (Ref.: Similarity to MIL-STD-701: Silicon Low Power Chopper Transistors) |
| • Resistor Chips |
| • Small Signal Diodes with power $\leq$1watt excluding Zeners (Ref.: Similarity to MIL-STD-701: Silicon Switching Diodes (listed in order of increasing tr)) |
| • General Purpose Silicon Rectifier Diodes and Fast Recovery Diodes (Ref.: Similarity to MIL-STD-701: Silicon Axial Lead Power Rectifiers, Silicon Power Diodes (listed in order of maximum DC output current), Fast Recovery Diodes (listed in order of tr)) |
| • Low Power Silicon Transistors with power $\leq$5watts at $25^{\circ}$ C (Ref.: Similarity to MIL-STD-701: Silicon Switching Diodes (listed in order of increasing tr), Thyristors (bi-directional triodes), Silicon PNP Low-Power Transistors (Pc $\leq$5 watts $T_A = 25^{\circ}$ ), Silicon RF Transistors). |
| • All other Microcircuits not included in Class 1 or Class 2 |
| • Piezoelectric Crystals |
| • Hybrids utilizing Class 3 parts |

TABLE 5.3-2. PART CONSTITUENTS SUSCEPTIBLE TO ESD

| Part Constituent | Part Type | Failure Mechanism | Failure Indicator |
|---|---|---|---|
| Film Resistors | Hybrid ICs:<br>Thick Film Resistors<br>Thin Film Resistors<br>Monolithic IC-Thin Film Resistors<br>Encapsulated Film Resistors | Dielectric breakdown voltage dependent-creation of new current paths<br>Joule heating-energy dependent-destruction of minute current paths | Resistance shift |
| Metalization Strips | Hybrid ICs<br>Monolithic ICs<br>Multiple Finger Overlay Transistors | Joule heating-energy dependent metalization burnout | Open |
| Field Effect Structures and Nonconductive Lids | LSI and Memory ICs employing nonconductive quartz or ceramic package lids especially ultraviolet EPROMS | Surface inversion or gate threshold voltage shifts from ions deposited on surface from ESD | Operational degradation |
| Piezoelectric Crystals | Crystal Oscillators | Crystal fracture from mechanical forces when excessive voltage is applied. | Operational degradation |
| Closely Spaced Electrodes | Surface Acoustic Wave Devices<br>Thin metal unpassivated, unprotected semiconductors and microcircuits | Arc Discharge melting and fusing of electrode metal | Operational degradation |

TABLE 5.3-2. PART CONSTITUENTS SUSCEPTIBLE TO ESD (Continued)

| Part Constituent | Part Type | Failure Mechanism | Failure Indicator |
|---|---|---|---|
| MOS Structures | MOS FET (Discretes)<br>MOS ICs<br>Semiconductors with metalization crossovers<br>Digital ICs (Bipolar and MOS)<br>Linear ICs (Bipolar and MOS)<br>MOS Capacitors<br>Hybrids | Dielectric breakdown from excess voltage and subsequent high current | Short (high leakage) |
| Semiconductor Junctions | Diodes (PN, PIN, Schottky)<br>Transistors, Bipolar Junction Field Effect Transistors<br>Thyristors<br>Bipolar ICs, Digital and Linear<br>Input Protection Circuits on:<br>Discrete MOS FETs<br>MOS ICs | Microdiffusion from micro-plasma secondary breakdown from excess energy or heat<br>Current filament growth by silicon and aluminum diffusion (electromigration) | Operational degradation |

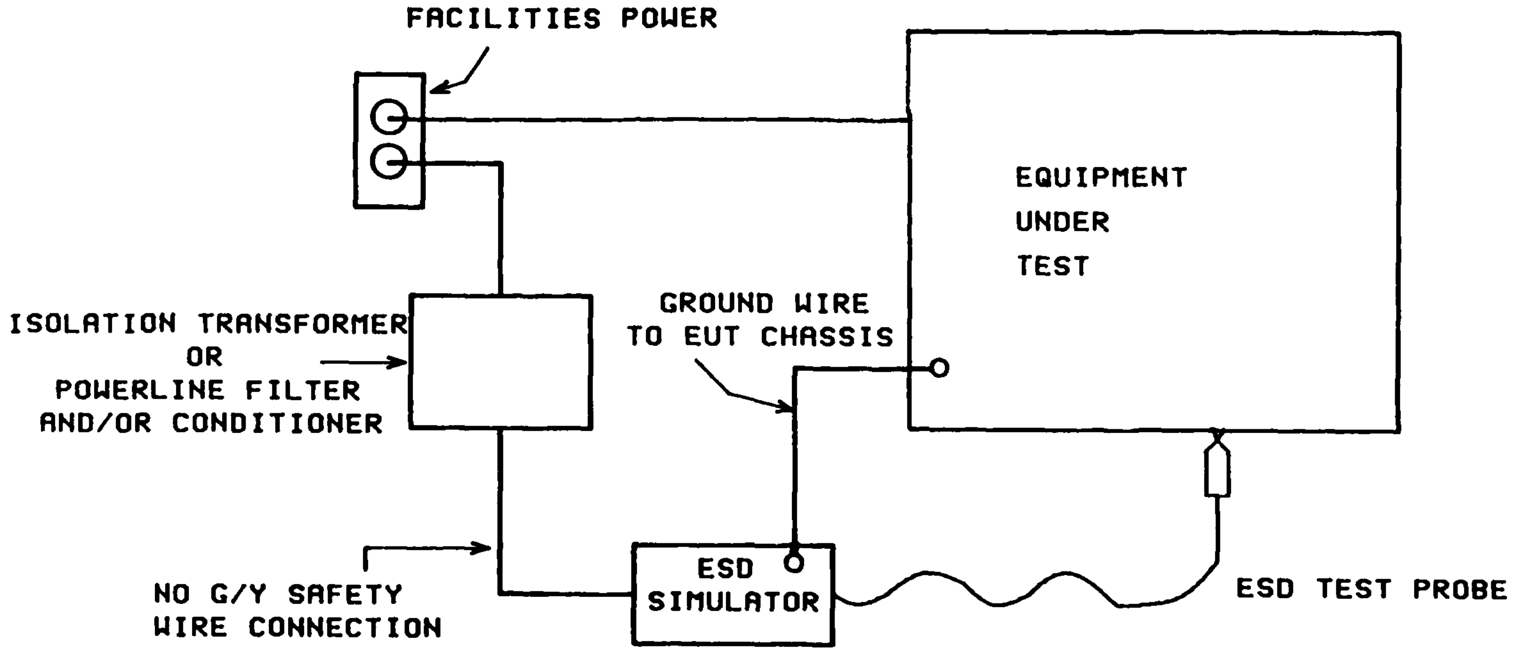


FIGURE 5.3-3. ESD DIRECT DISCHARGE EQUIPMENT CONFIGURATION

TABLE 5.4-1. PREDICTION OF RADIATED EMISSIONS

| FREQ | 1.<br>Cn dBuV/MHz | 2.<br>$T_F$ | 3.<br>ANT. F. | 4.<br>N | 5.<br>D | 6.<br>HEIGHT | 7.<br>RESULT |
|---|---|---|---|---|---|---|---|
| 1.58 MHz | 193.7 | -34 | -13.8 | 0 | 0 | 0 | 145.9 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

The dB values in columns 1 through 6 are now added to obtain the result in column 7, 145.9 dB$\mu$V/meter/MHz. This value can be converted to a radiated field strength:

$$E = 10^{(145.9/20)} \ \mu V/meter/MHz$$

or

$$E = 19.7 \ V/meter/MHz$$

To arrive at the magnitude of the field threatening a broadband device, the frequency domain plot of figure 5.2-1 can be integrated over the frequency range of interest. Piecewise integration from DC to 1.58 MHz yields a value of 31.2 volts per meter. This value is the field value that would be seen by a device which cuts off sharply at 1.58 MHz. Continuing the integration from 1.58 MHz to 159 MHz gives an additional field value of 1,550 volts per meter as the contribution from this portion of the spectrum. The total field is the sum of the two piecewise integrations and is then 31.2 + 1,550 = 1,581 volts per meter per 159 MHz. This is the field which would be seen by a broadband device having response from very low frequencies up to 159 MHz. Above 159 MHz, the field strength decreases at a rate of 40 dB per decade, and the contribution from this part of the spectrum is negligible.

## 5.5. Prediction of Voltage Induced on a Susceptible Circuit

The next part of the problem is to calculate how much voltage might be induced on a susceptible circuit by the field calculated above. For the susceptible circuit a printed circuit board will be used into which a loop area has been inadvertently designed. The loop acts as an antenna which responds to the field calculated above. Assumed are loop dimensions of 4 inches by 6 inches, which could be created by a trace around the periphery of the board. The induced voltage as a function of field strength is given by:

$$V(volts) = \frac{2\pi}{\lambda} E \ N \ A \cos\theta \qquad (16)$$

E is the field strength; N is the number of turns in the receiving loop; A is the area of the loop in square meters; lambda is the wavelength; and theta is the angle of the loop with respect to the radiating field. (Theta is usually taken to be zero for a worst case estimate.)

An effective way of combining the broadband field generated by the pulse with the response of the loop from DC to 159 MHz is to plot the field and the response in dB on semilog paper, as in figure 5.5-1. No values are shown above 159 MHz because the induced voltage above that point is negligible. The generated E field is shown in the uppermost curve and has frequency distribution as in figure 5.2-1. The loop response with an applied field of 1 volt per meter is shown in the lower curve and shows a linear response with frequency with a

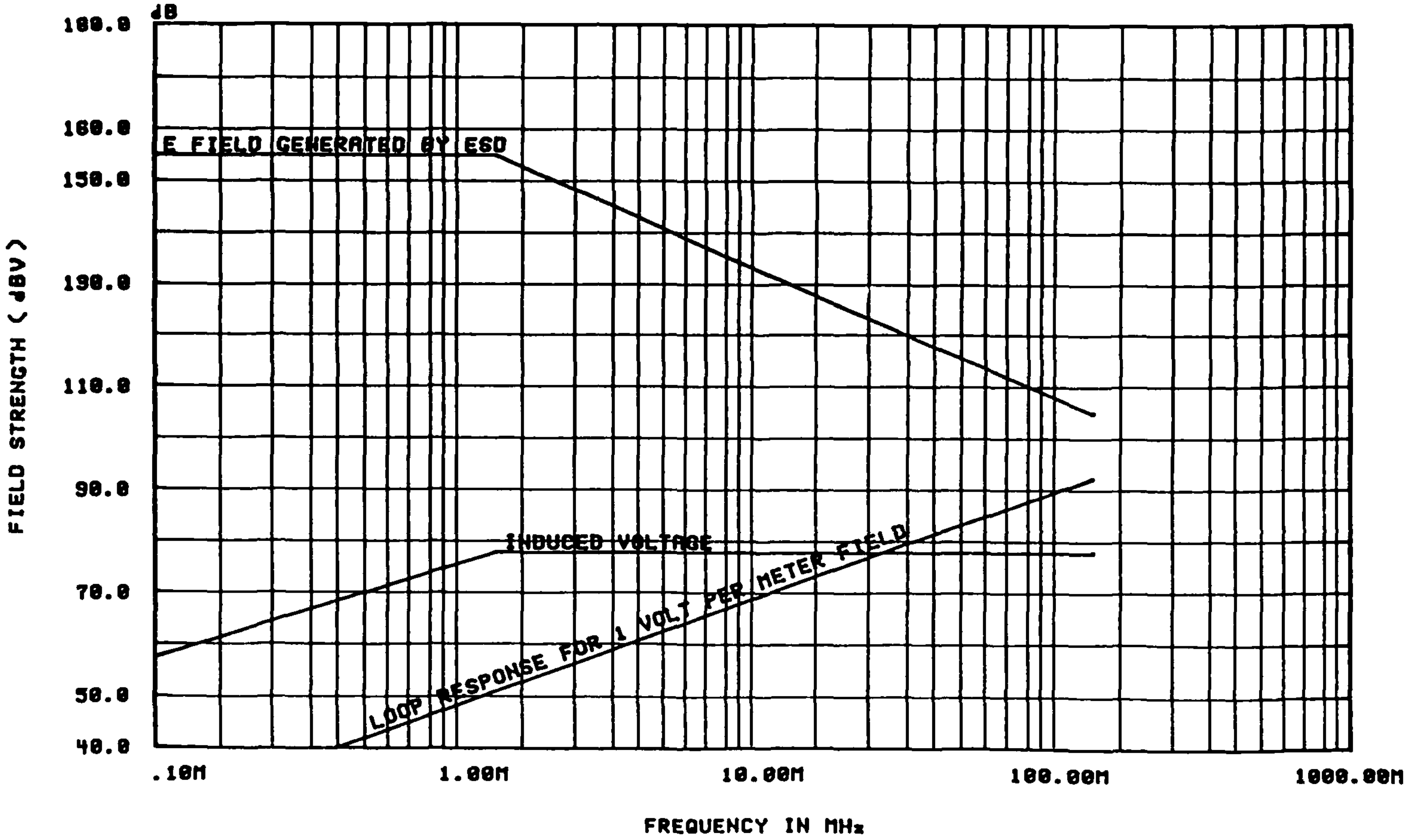


FIGURE 5.5-1. INDUCED VOLTAGE ON A LOOP FROM ESD

slope of 20 db per decade. The curve for the induced voltage in the loop is found by combining the applied field curve and the response curve. From 1.58 MHz up, the curve shows a steady value of 7.9 millivolts per MHz.

When the curve in figure 5.5-1 is integrated over the bandwidth to 159 MHz, the total voltage to which a broadband device would be exposed is about 1.25 volts, which is in the upset range for TTL devices.

In the analysis it was assumed that the receiving loop was unshielded. Shielding of the susceptible circuit will normally provide enough attenuation to reduce the induced voltage to a non-threatening level. However, an increase in the original 12 kV discharge voltage, a failure of shielding, a resonance condition in the susceptible circuit, or a decrease in the distance from the discharge to the susceptible equipment, can increase the induced voltage to the upset or damage levels.

Testing for radiated induced ESD is performed on installed systems using an ESD simulator while operating the systems under test and looking for upset conditions or damage conditions.

## 5.6. ESD Induced Voltages on Cables

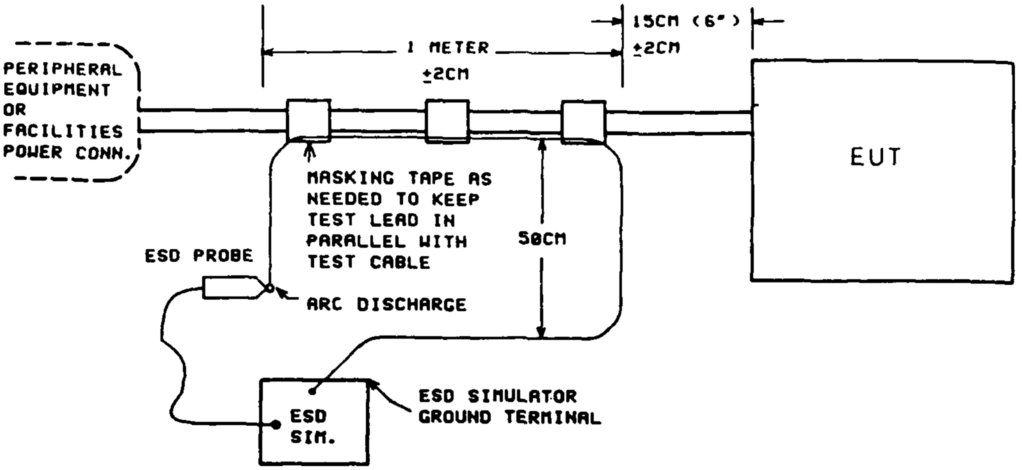
When a discharge occurs to a cabinet, which is connected to a shielded cable, some of the discharge current flows to ground via the cable shield. The noise of the discharge can be coupled to the cable center conductor through the transfer impedance of the cable, or by direct coupling to an exposed center conductor (in the case of improperly terminated shields), or directly through the *shield itself. Figure 5.6-1 shows a test arrangement* used for the ESD testing of cables. In an installed system, the ESD simulator voltage would be applied near the connectors at each end of a cable and to as much of the shielding between as is accessible.

In tests by the 3M Company, voltages larger than 500 volts could be induced on a center conductor by ESD if one end of the shield was unterminated. When the shield was terminated with a pigtail connection, the induced voltage was reduced to 16 volts. When the proper 360° backshell termination was made, a further reduction to just over a volt occurred. These results point out both the threatening nature of ESD and the necessity of proper cable shield termination.

## 5.7. Summary of ESD Prediction Technique

The procedure just given falls into four parts. First, the field at a distance of one meter from the discharge is calculated. Later, if desired, the field strength can be adjusted for distances other than one meter. A starting point for this field calculation is the information contained in figure 5.2-1.

Next, the susceptibility of the threatened circuit is calculated. Then the field and the susceptibility curves are combined to produce a resultant curve of induced voltage versus frequency. Graphical combining of the curves is most readily performed on a semilog scale as shown in figure 5.5-1.



NOTES:

1. TEST LEAD PLUS LOOP SHOULD BE 1 METER AWAY FROM ANY CONDUCTING SURFACE INCLUDING CEMENT FLOOR. A WOOD TABLE IS AN IDEAL TEST PLATFORM.
2. WHEN TEST CABLE IS LESS THAN 1.15 METERS IN LENGTH, THEN TEST PARALLEL SHALL BE SHORTER AND STARTED A MINIMUM OF 5CM (2") AWAY FROM EUT CONNECTOR.

FIGURE 5.6-1. ESD TEST CONFIGURATION (CABLE INDUCED)

The voltage induced in the susceptible circuit is found by converting from dB microvolts per meter per MHz to volts per meter per MHz.

Finally, the average value of the induced voltage over the frequency range is found by integrating over the entire spectrum of interest.

After appropriate adjustments are made for shielding or other attenuation factors, the induced voltage can be compared to the upset and damage levels of the threatened circuit or system.

## 5.8. ESD Testing Recommendations

It is recommended that ESD tests be performed because of the flight critical nature of new systems and the high susceptibility of broadband logic devices to ESD phenomena. The specific ESD test recommendations for flight critical systems follows.

Equipment, systems, and installed systems should be ESD tested according to table 5.8-1.

A soft failure is one which causes an alteration of data or missing data. A hard failure is one which requires a reset of equipment. Damage requires repair or replacement of a system, subsystem, or component.

All tests should start at the 2 kV level and should be advanced in 1 kV increments until a failure occurs (or the specified level is reached without failure).

TABLE 5.8-1. ESD TESTS

| Failure Mode | ESD Test Level | Simulator | Circuit Values |
|---|---|---|---|
| Soft | 8 kV | 150 pf | 1200 ohms |
| Hard | 12 kV | 150 pf | 1200 ohms |
| Damage | 25 kV | 150 pf | 1200 ohms |

## 6. CONDUCTED FAST TRANSIENTS ON POWER LINES

When an aircraft is on the ground and being serviced, it is possible that fast transients will be introduced on the primary power lines. The connection and disconnection of Auxiliary Power Units (APU) and switch-over from the APU to aircraft power are likely sources of these transients. In flight the operation of other on-board equipment may cause similar disturbances.

Typical power line transients are described in two comprehensive military standards. MIL-STD-461C defines pulse shapes, amplitudes, and time characteristics. MIL-STD-462 gives detailed test procedures. The applicable test is Conducted Susceptibility, CS06. A review of this specification is recommended.

Two types of transients are described. One is a heavily damped spike which starts out with a positive polarity, goes negative, and then rapidly decays to zero. The second transient is a trapezoidal pulse. Tests are conducted with pulse times of both 0.15 microseconds and 10 microseconds. The pulse amplitude is specified as 200 volts. These transients are shown in figure 6-1.

Although the military specification states that these pulses are to be applied to equipment and subsystem AC and DC power lines, such testing may be inappropriate in some cases. For example, low voltage DC power supplies may be unable to tolerate 200 volt spikes applied to their input leads. In recognition of these difficulties, MIL-STD-462, Notice 2, states "A detailed test procedure shall be included in the test plan to provide a practical measurement on the item to be tested, as the specified procedure often cannot be accomplished."

The CS06 tests are most appropriate for 28 Volt, Direct Current and 115 Volt, Alternating Current, 400 Hz primary power lines.

RTCA/DO-160B describes rather similar power line transients and test procedures. A thorough review of Section 17 of that document is recommended.

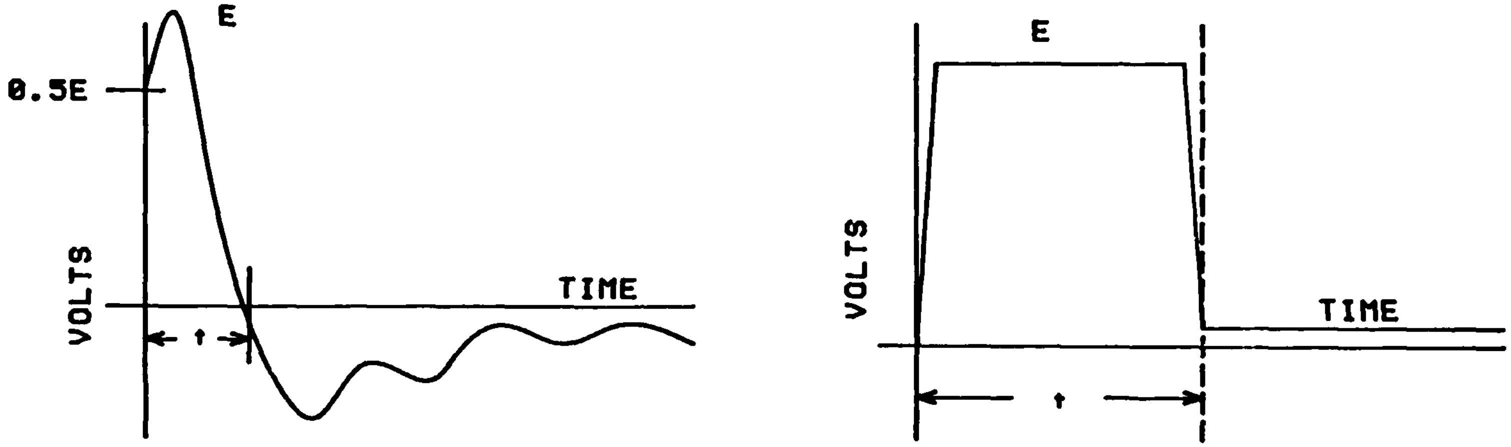
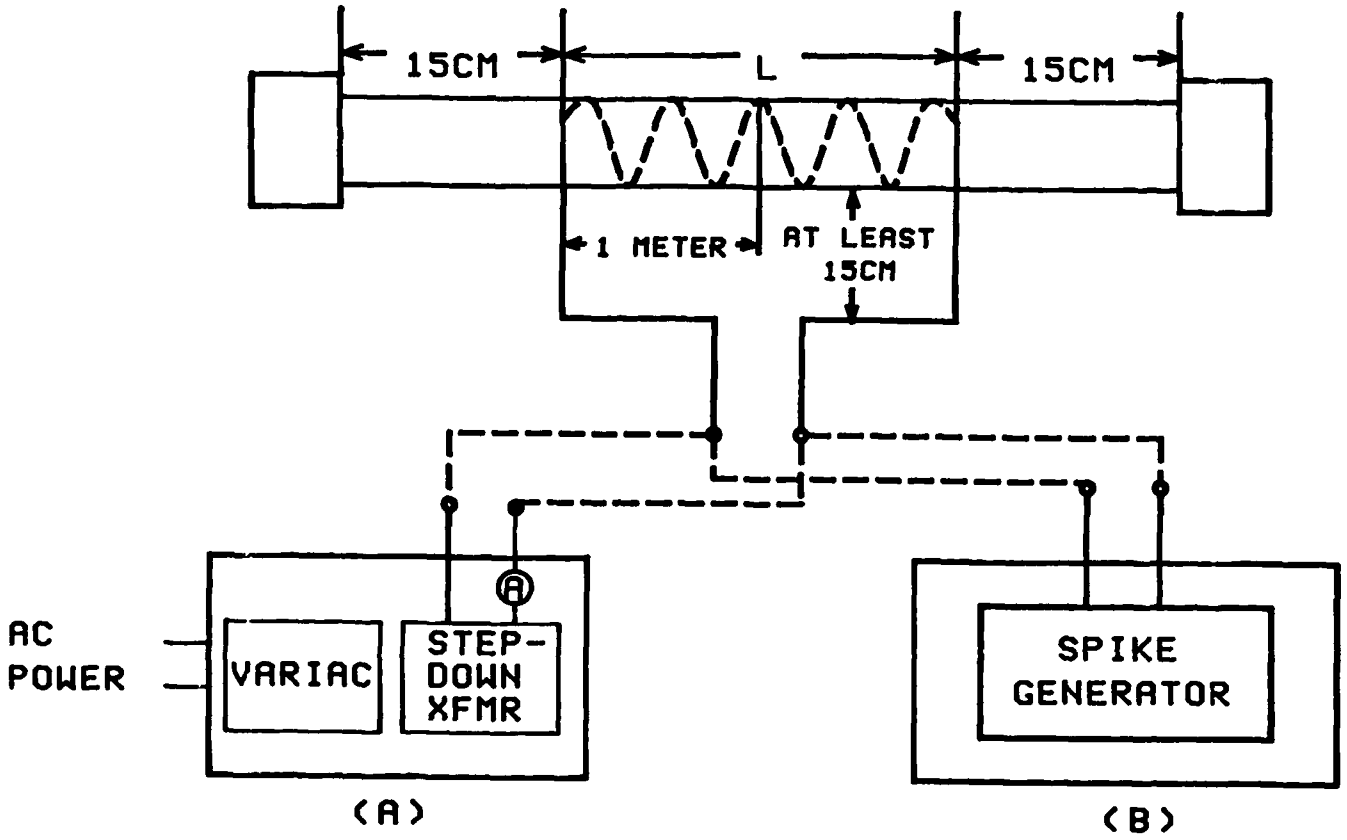


FIGURE 6-1. POWER LINE TRANSIENT TEST WAVESHAPES

## 7. RADIATED SUSCEPTIBILITY TO MAGNETIC INDUCTION FIELDS

The same transient spikes described in the previous section are also applied, under MIL-STD-461C, RS02, as magnetic induction fields to cables and equipment. The transient spikes must not cause "malfunction, degradation or deviation from specified indications..."

For these tests, a wire is wrapped around either cables or equipment, as shown in figures 7-1 and 7-2. The specified test spikes are applied from the spike generator. For complete details, see MIL-STD-461C and MIL-STD-462.



NOTE:

(1) L SHALL BE THE LENGTH OF THE CABLE IN THE ACTUAL INSTALLATION OR 1.5 METERS, WHICHEVER IS LESS.

FIGURE 7-1. RADIATED SUSCEPTIBILITY, MAGNETIC INDUCTION FIELD, CABLE TEST

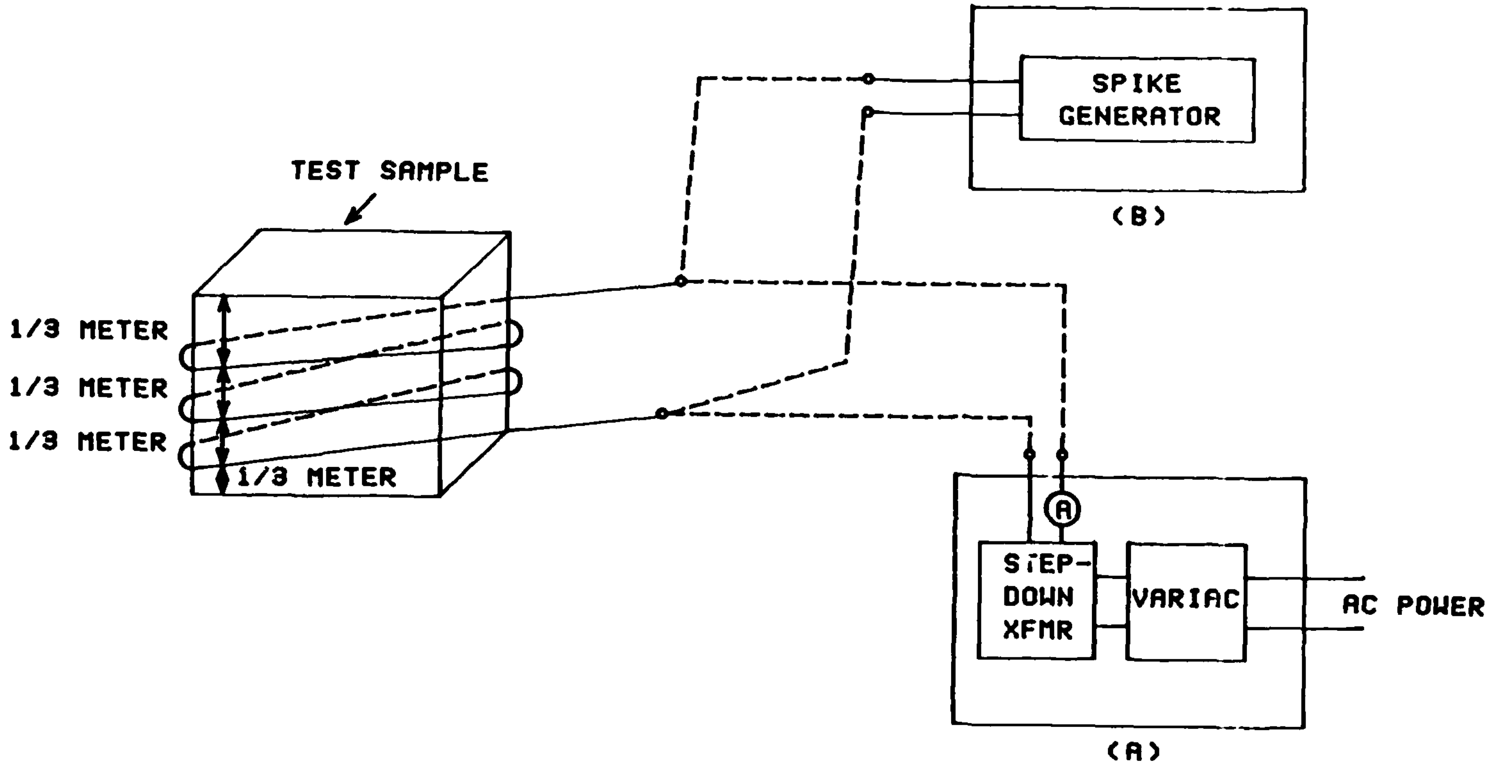


FIGURE 7-2. RADIATED SUSCEPTIBILITY, MAGNETIC INDUCTION FIELD, CASE TEST

## 8. MIL-STD-461C EMP TESTS

MIL-STD-461C defines Electromagnetic Pulse (EMP) pin level test limits under Conducted Susceptibility CS-10 and EMP cable test limits under Conducted Susceptibility CS-11. MIL-STD-462 gives detailed test procedures. A review of these references is recommended for a thorough understanding of these tests.

Briefly, a pin level test involves the direct connection of a test signal generator to a pin of a cable connector, followed by application of the test signal, and observation of the equipment under test for malfunction or degradation.

The cable test, Bulk Cable Injection (BCI), calls for inducing a specified current on a cable bundle or shield and again observing the equipment under test.

# 9. PROTECTIVE MEASURES

This section briefly describes various ways in which equipment and systems can be protected from the effects of fast transients.

Shielding is the most fundamental way of protecting both equipment and cables. All multiconductor cables, which carry signals that could be affected by transients, should be shielded. Other circuits, which can be regarded as generators of transient energy, should also be shielded to reduce their radiated emissions.

Particularly critical data can be transmitted on shielded twisted pairs. The twisting provides a measure of shielding effect by itself, and a single or even double shield provides further protection.

Coaxial lines with a single center conductor are frequently used. The braid-over-foil type is most effective. The foil provides nearly the effect of a solid outer shield, and the braid provides both physical protection and additional shielding. The type of fold is critical to the shielding effectiveness: a longitudinal "z-fold" or cigarette type fold is best. Spirally wrapped foil shields are less effective. The most effective coaxial cable shield is a solid metal outer conductor, but because of its lack of flexibility, it is ordinarily only used in short lengths within the avionic systems.

The method of shield termination is critical to maximizing the effectiveness of the shielding. All shields should be terminated with a $360^0$ connection of the shield to the back shell of the cable connector. Experiments have shown a 30 dB or more degradation of shielding when a "pigtail" connection as little as 1 inch in length is used instead of the $360^0$ connection.

Equipment case shielding is another line of defense against fast transients. Metal boxes provide effective shielding except against low frequency magnetic fields; however, holes, slots, seams, and apertures of any kind can allow entry of energy. In the case of ESD, some of the energy is in the 10 to 1000 MHz region and even fairly small apertures can degrade the shielding effectiveness.

A one-inch diameter hole has an attenuation of 40 dB at 60 MHz. This value scales downward (less attenuation) with increasing frequency at a rate of 20 dB per decade. Seams and slots can actually act as antennas. If the length of a slot or seam is one-half wavelength for an interfering signal, the slot or seam can resonate (like a magnetic dipole) and transfer signals with no attenuation at the frequency of resonance.

Filtering is another form of protection from fast transients. The energy in fast transients is primarily at higher frequencies. Low-pass filters which pass low frequencies and reject high frequencies can be effectively used on power lines and data lines to limit both radiation and reception of transient energy.

The cutoff frequency of the filter must be high enough to allow passage of the desired power or data frequency and low enough to prevent the flow of the transient energy. An example was given earlier in this chapter of the selection of a cutoff frequency in a low-pass filter. Filters can be designed in the form of discrete components. Filters may also be designed into the cable connectors. For many applications, a series inductance and a shunt capacitor provide adequate attenuation.

Ferrite beads placed over the end of a wire or cable can also provide a type of filtering. The common mode (line to ground) impedance is raised by the bead. For initially low impedance circuits, 6 to 10 dB of common mode attenuation results at frequencies from 10 to 100 MHz.

Various solid state protection devices exist which generally shunt transient energy to ground, while interrupting the normal flow of power or data for only brief periods. Variously known as transzorbs, surge suppressors, and varisters, these devices can all be considered as switches which are automatically operated by excessive voltage. They are connected in shunt-to-ground, and normally present a high impedance to the power or data line. When operated by the presence of the transient, they change state, go to a very low impedance, and short-circuit the line to ground. Designs are available in both unidirectional and bidirectional versions.

ESD protection requires attention to equipment case shielding. Control knobs and shafts can be grounded to the equipment case. This grounding will prevent entry of transient energy inside the case and will force the energy to flow on the outside to ground.

Attention should also be given to materials selection both in the aircraft structure and the equipment. Some materials, particularly plastics, are more apt to promote charge separation and accumulation, leading to ESD.

High voltage DC power supplies (found in video display units) are sources of charge and should be completely shielded to prevent charge transfer to nearby objects.

Keyboards on data entry units are often points of entry for ESD. Membrane- type keyboards are particularly vulnerable, but shielding can be incorporated between the keyboard and the sensitive components beneath.

# BIBLIOGRAPHY

Air Force Systems Command Design Handbook, AFSC DH1-4, Electromagnetic Compatibility, Wright Patterson Air Force Base (AFB).

Electrical Overstress/Electrostatic Discharge Symposium Proceedings, EOS-1, EOS-2, EOS-3, EOS-4, and EOS-5. Reliability Analysis Center, Rome Air Development Center, Griffiss AFB, NY 13441.

ESD Control in the Manufacturing Environment, Department of Defense

IEEE Transaction on Electromagnetic Compatibility: Many references available since 1958.

IEEE International Symposium on Electromagnetic Compatibility: Many annual references available since 1969.

Mardiguian, Michael, Electrostatic Discharge: Understand, Simulate and Fix ESD Problems, Interface Control Technologies, Library of Congress Number 85-80686, ISBN 0-932263-27-5.

McConnell, Roger A., DOT/FAA/CT-87/19, Avionics System Design for High Energy Fields.

MIL-B-82547, Electromagnetic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies, and Equipment, (Excluding Electrically Initiated Explosive Devices).

MIL-STD-461-C, Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference.

MIL-STD-462, Electromagnetic Interference Characteristics, Measurements of.

Military Handbook DOD-Hdbk-263, Electrostatic Discharge Control Handbook for the Protection of Electrical and Electronic Parts, Assemblies and Equipment.

National Communications System, NCS TIB 85-10, Volume 1, Electromagnetic Pulse/Transient Threat Testing of Protection Devices for Amateur/Military Affiliate Radio System Equipment.

Radio Technical Commission for Aeronautics, RTCA/DO-160B, Environmental Conditions and Test Procedures for Airborne Equipment.

R&B Enterprises, EMP Testing Handbook, R&B Enterprises, EMP Division, 20 Clipper Road, West Conshohocken, Pa. 19428.

# GLOSSARY

BROADBAND. A frequency spectrum which is wide compared to the bandwidth of the device used to detect it.

DECIBEL. A dimensionless unit for representing the ratio of values of power or voltage.

dBμV. Decibels referred to one microvolt. Zero db represents one microvolt.

FALL-TIME. The time required for pulse amplitude to go from a predefined magnitude to a given level.

FOURIER TRANSFORM. A mathematical method for deriving the frequency spectrum from a time dependent function.

HARD FAILURE. A failure that requires a reset of the equipment.

JOULE. A unit of energy equal to one watt-second.

LOW-PASS FILTER. An electrical circuit which allows the passage of low frequencies and prevents the passage of high frequencies.

PIN LEVEL TEST. An EMC test in which voltage or current is applied directly to a conductor at a connector pin.

Q. The quality factor of a resonant circuit which is the ratio of the energy stored to the power dissipated per cycle.

RESONANCE. Resonance occurs in an electrical circuit when the energy stored in the inductance is equal to the energy stored in the capacitance.

RISE-TIME. The time required for a voltage pulse to reach a predefined percentage of the amplitude from a given level.

SHIELDING. Any metallic structure such as the aircraft fuselage or the woven braid on a cable that provides protection against electromagnetic fields.

SINUSOID. A wave form that follows the mathematical values of a sine function.

SOFT FAILURE. A failure which causes an alteration of data or missing data.

UPSET. A condition in which the state of a digital device is unintentionally altered, but may be restored by automatic means or by operator intervention.

## ACRONYMS AND ABBREVIATIONS

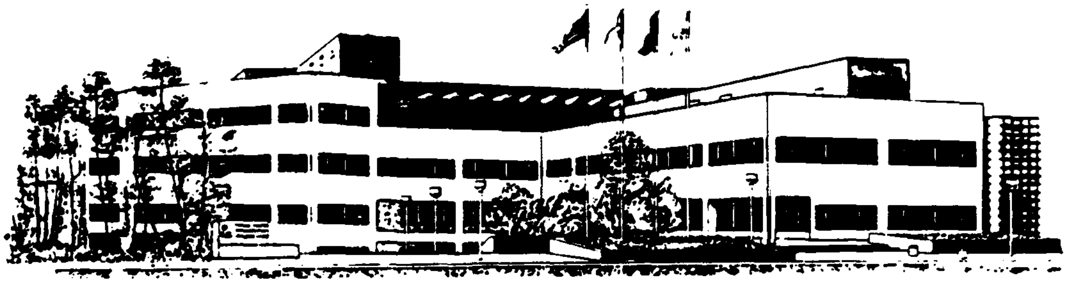
| | |
|---|---|
| AC | Alternating Current |
| APU | Auxiliary Power Units |
| BCI | Bulk Cable Injection |
| CMOS | Complimentary Metal-Oxide Semiconductor |
| dB | decibels |
| DC | Direct Current |
| DOD | Department of Defense |
| EMC | Electromagnetic Compatibility |
| EMCad$^{tm}$ | Electromagnetic Computer aided design |
| EMP | Electromagnetic Pulse |
| ESD | Electrostatic Discharge |
| kHz | Kilohertz |
| MHz | Megahertz |
| NEMP | Nuclear Electromagnetic Pulse |
| pf | picofarad |
| R-C | Resistor-Capacitor |
| RTCA | Radio Technical Commission for Aeronautics |
| TTL | Transistor-Transistor Logic |

U.S. Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II DIGITAL SYSTEMS VALIDATION

## CHAPTER 13 LIGHTNING STUDIES



PREPARED BY:

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

PREPARED FOR:

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

# LIST OF ILLUSTRATIONS

Figure Page

# LIST OF TABLES

# 1. INTRODUCTION

While the effects of lightning strikes on metal aircraft are considered minimal, there is a greater threat to advanced technology aircraft. There are two major reasons for this increased threat. Digital electronic components are more susceptible to electrical transients than analog systems in older aircraft. Also, advanced composite structural materials offer less electrical shielding than metallic structures. Both of these factors reduce the inherent protection of electronic/electrical systems found on previous technology, all-metal aircraft.

Competition in the marketplace for aircraft sales and the increasing cost of fuel is developing pressure on manufacturers to employ advanced technology electronic equipment and materials, such as bonded honeycomb, kevlar, fiberglass, or Graphite Epoxy (G/E), in the next generation of aircraft. This is evident both in large transport and in general aviation aircraft currently under development. Several general aviation aircraft that employ advanced technology are nearing or are in the certification process. These include the Beech "Starship," Lear Fan, and AVTEK-400. In addition to the all electric engine control (Pratt & Whitney 2037) for the Boeing 757, transport aircraft manufacturers are researching the use of advanced composite structures, digital data busses (beyond ARINC 429), and all-electric systems.

Advanced technology materials and new structural fabrication methods, such as using adhesives in place of fasteners to minimize drag, reduce manufacturing costs as well as corrosion and fatigue. Several potential problems have prevented widespread use of the new structural technology. These include the variability of: lightning protection, static electrification, Electromagnetic Compatibility (EMC), mechanical and electrical parameters, impact resistance, effect of environmental factors, and production controls.

This chapter addresses the topic of lightning studies and the impact of lightning strikes to aircraft and digital systems.

Section 2 outlines some of the problems associated with the use of digital systems and composite materials in advanced technology aircraft. Currently accepted information about lightning current waveforms is reviewed. The lightning environment, which an aircraft might be expected to encounter, is discussed. A few examples of lightning effects on aircraft systems are given.

Section 3 covers the design approach to lightning indirect effects protection. A design margin must be established. Requirements for grounding and bonding must be taken into account. Preferred methods for equipment installation and cable routing to provide optimum protection from Electromagnetic (EM) hazards are reviewed.

Test methods for verification of protection design are reviewed in section 4. These test methods include a variety of lightning simulation techniques and equipment bench test techniques. Several simulation techniques are discussed and a comparison of test results for four methods is given. Verification of data quality is an important aspect of these test methods.

Analysis techniques are used to validate experimental results. Computer modeling methods are covered in section 5. Several techniques must be modified to be valid for composite structures where the dominant coupling mechanism is dependent on the resistance of the structure. The capabilities of several computer codes useful for predicting EM coupling due to lightning are summarized.

Section 6 contains worked examples to illustrate prediction of EM coupling to wiring. The examples cover very simple techniques as well as the procedure for a more detailed vehicle analysis.

# 2. BACKGROUND

## 2.1. History

Aircraft are exposed to a wide variety of EM environments from onboard and external sources including the following major items:

- The electrical power and electronics equipment often cause electric currents to flow in the structure, if not by design, perhaps through equipment faults or short circuits.
- Lightning strikes to an aircraft result in large currents of short duration. These currents may flow in the structure and in any of the metallic plumbing, control cables, or wiring for the electrical/electronic systems.
- Antennas on the aircraft and nearby high energy Radio Frequency (RF) sources may cause large RF currents in the structure.

Lightning is the most severe of these EM environments. Direct strike lightning currents may be as high as 200 kA and the rate of rise may exceed 100 kA per microsecond. The effects of such currents will be subsequently discussed. Power system and electronic fault currents may reach a few thousand amperes. RF current density may reach a few tens of amperes per meter. Lightning and electric circuit faults act upon a small point of contact; therefore, the structure could be damaged at entry points. The RF currents are not likely to result in structural damage, but could cause a functional disruption of digital electronic circuits and possibly of analog circuits as well.

Aircraft lightning strikes produce two types of effects.

- Direct effects: Physical damage from arcing and sparking.
- Indirect effects: Disruption of the electronic/electrical systems from electrical transients in the wiring and structural elements.

The trend in avionic/electrical equipment toward digital circuits having lower operating voltage and power levels adds to the concerns regarding protection against the indirect effects of lightning strikes and static electrification. The poor (lower) conductivity of composite materials and the bonds between structural members make it difficult to obtain the 2.5 milliohm bonding and grounding required by current military specifications (MIL-B-5087B(ASG), 1970). If the 2.5 milliohm specification were applied, the assessment indicates that all electrical systems would be safe.

Structures composed of many of the newer materials will be far more resistive than the present 2.5 milliohm requirement. Kevlar is an insulator and G/E structures may have resistances of a few ohms. Designs using these materials should allow the addition of enough metal so that protection against lightning strikes may be achieved. These designs should also allow the addition of metallic pathways in the grounding and bonding systems so that onboard systems will function properly in the presence of currents anticipated from normal or fault conditions in onboard equipment.

There are also concerns about potential interference between different onboard digital systems and sources of Electromagnetic Interference (EMI). The EM shielding effectiveness of a composite fuselage without seams or joints is one to two orders of magnitude less than that of an aluminum fuselage. Seams and joints reduce the shielding to a practical upper limit of 25 to 40 dB depending on size and number of seams and joints. The EM Compatibility (EMC) between digital and RF circuits using the structure as a return path is more critical for new aircraft than for older aircraft.

Since advanced aircraft digital electronics operate at a few volts compared with a few tens of volts for analog systems, the design margin in future advanced aircraft electronic systems may be reduced by two to three orders of magnitude. (See section 3.1.) Considerable design efforts may be required to accomplish the protection for these advanced technology aircraft because of the reduced margins of safety between the EM induced transients (stress) and the ability of future technology equipment to withstand these transients (strain). Figure 2.1-1 shows the problems associated with EM protection of digital systems and changing electrical parameters when replacing metal structure with composite materials. Figure 2.1-2 indicates the variability in transfer impedance of various materials.

The characteristics of electrical transients induced in aircraft wiring and avionics systems are affected by the system response of the entire aircraft to the lightning stimulus. Induced coupling and susceptibility tests may be conducted on electrical hardware and associated wiring at the subsystem level. Determination of the voltage and current levels induced into the equipment by a lightning strike must take into consideration the structural interaction with the arc, the subsequent coupling of the magnetic and electric fields generated by lightning currents on the external surfaces, and coupling to internal wiring and equipment. The presence of an aircraft in the lightning channel may modify the natural lightning current waveform as a result of the resonant responses of the aircraft structure.

The demonstration and validation of the lightning/static electrification protection design is more critical for the new materials and electronics technology than for older aircraft technology. Extrapolation of prior protection designs on metal aircraft to those on advanced technology aircraft is not valid because the protection technology is completely different. Very few protection measures were required to protect older metal aircraft from indirect effects.

| IMPACT ON EM PROTECTION FROM REPLACING METAL STRUCTURE WITH COMPOSITES | | | IMPACT ON ELECTRICAL PARAMETERS FROM REPLACING METAL STRUCTURE WITH COMPOSITES | | | |
|---|---|---|---|---|---|---|
| **MINOR** IMPACT ON PROTECTION METHODS | **SUBSTANTIAL** IMPACT ON PROTECTION METHODS | | **CONDUCTIVITY** - STRUCTURAL END-TO-END RESISTANCE MUST BE SMALL TO PROVIDE A PATH FOR LIGHTNING CURRENTS. | **TRANSFER IMPEDANCE** - SHIELDING EFFECTIVENESS PROVIDED BY STRUCTURE WILL DEPEND ON MATERIAL TRANSFER IMPEDANCE. | **JOINT IMPEDANCE** - GOOD ELECTRICAL CONTACT AT JOINTS IS NECESSARY TO PREVENT ARCS AND SPARKS. | **GROUNDING** - GROUND CONNECTIONS MUST ACCOUNT FOR IR DROP IN STRUCTURAL MATERIALS AND BETWEEN EQUIPMENT. |
| | | LIGHTNING DIRECT EFFECTS | | | | |
| ▨ | | STRUCTURAL EFFECTS | ▨ | | | |
| | ▨ | FUEL SYSTEMS | ▨ | | ▨ | ▨ |
| | ▨ | LIGHTNING INDIRECT EFFECTS | ▨ | ▨ | ▨ | ▨ |
| | | ANTENNA PERFORMANCE | | | | |
| | ▨ | HF AND LF | | | ▨ | ▨ |
| ▨ | | VHF - L BAND | | | ▨ | ▨ |
| | ▨ | ABOVE L BAND | ▨ | | ▨ | |
| ▨ | | STATIC ELECTRICITY | | | ▨ | |
| | ▨ | EMI/EMC/EMP | ▨ | ▨ | ▨ | ▨ |
| | ▨ | POWER SUBSYSTEM | ▨ | | ▨ | ▨ |

NOTE: ▨ Shaded area indicates impact.

FIGURE 2.1-1. PROBLEMS ASSOCIATED WITH PROTECTION OF DIGITAL SYSTEMS IN ADVANCED TECHNOLOGY STRUCTURES

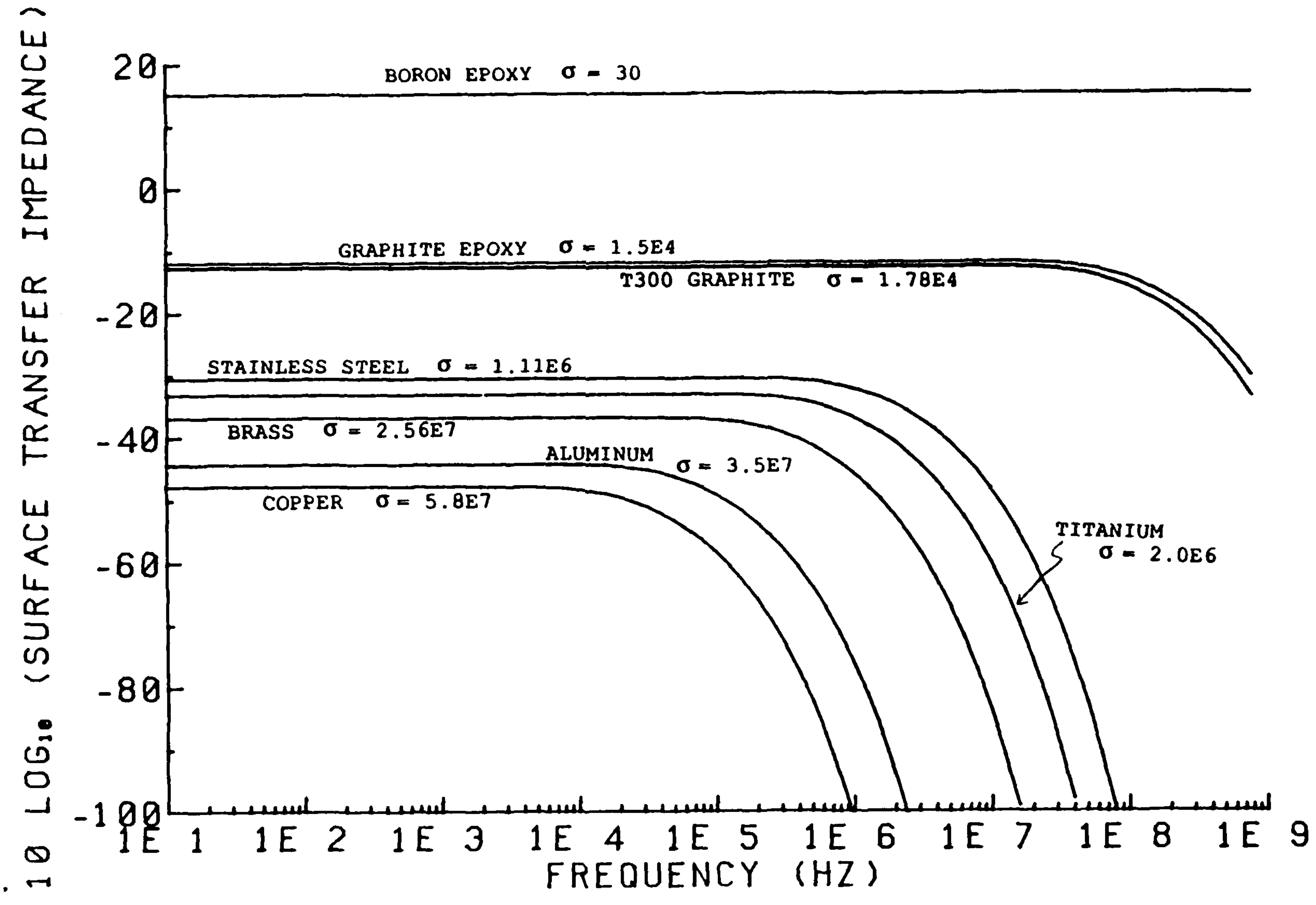


FIGURE 2.1-2. SURFACE TRANSFER IMPEDANCE FOR VARIOUS MATERIALS

The design margins did not exist for the older designs because of prior experience with the inherent insensitivity of metal aircraft to lightning strikes. Advanced technology aircraft are judged to have three to four orders of magnitude less design margin based upon the reduced shielding effectiveness of the fuselage and the sensitivity of the digital electronics (Sommer, 1981). It is natural to question the protection designs with such a great change in design margins.

Because of the increased potential for damage to electronic systems in advanced technology aircraft, simulated lightning tests must be performed to verify the adequacy of the design measures utilized to prevent serious loss or damage resulting from a lightning strike. It is recognized that the necessary protection verification test cannot be performed as a go/no-go test at full lightning threat levels, discussed in section 2.2, for several reasons as follows:

- The required electrical storage capacity in the lightning simulator would be excessive for a 200,000 amp discharge through an aircraft.
- The required fast rise-time (2.0 x $10^{11}$ amps/second) for a 200,000 amp discharge could not be attained.
- The discharge currents and charge densities around the aircraft would be different in flight.
- There is no predictable method to update test results for airplane modifications.
- The perceived lightning threat may be changed in the future as more data become available through the efforts of the National Acronautics and Space Administration (NASA), Federal Aviation Administration (FAA), and others investigating the effects of lightning on aircraft in flight.

Lightning and static electrification protection design and demonstration of the design for aircraft and ground based systems are current topics for considerable technical research and development. The electrical impedance of a full-scale aircraft precludes the use of severe lightning current pulses such as those used for component indirect effects tests. Consequently, lower level current pulses have been used to evaluate the transients produced by a lightning strike. Lightning simulation testing is a very challenging technical area because it is very difficult, if not impractical, to conduct a full-scale simulated lightning test on large aircraft (MIL-STD-1757 and report of SAE Committee AE4L, 1978). The energy storage and electrical circuits capable of delivering a full-threat 200 kA peak current require simulator voltages greater than can be achieved in air (in excess of 2 million volts for a 25-foot long aircraft). Facilities to generate these conditions presently cost over a million dollars. Even with costly tests, there are no methods to update the results for airplane modifications, or methods to incorporate changes in the lightning threat. For the last several years there have been regular conferences dedicated to these topics. (See International Aerospace and Ground Conference on Lightning and Static Electricity in the Bibliography.)

Because of the practical considerations regarding simulator limitations, several different simulation test techniques are used for lightning and static electricity design demonstrations on full vehicles. The simulation and analysis methods are specialized to the unique character of lightning attachment, vehicle charging, high arc current flow, and vehicle discharging.

There are several variants on the high current pulse simulation techniques that are used for full vehicle lightning tests. The four principal lightning simulation test techniques are:

- Low-level swept Continuous Wave (CW).
- Low-level fast rise pulse.
- Full threat fast rise pulse.
- Shock-excitation.

Included in the accuracy of technique are the analytical models and computations used to verify and validate the test data. For some methods, analytical techniques provide extrapolation of the test data to other environments and guidance for modifications of the aircraft design.

## 2.2. Lightning Environment

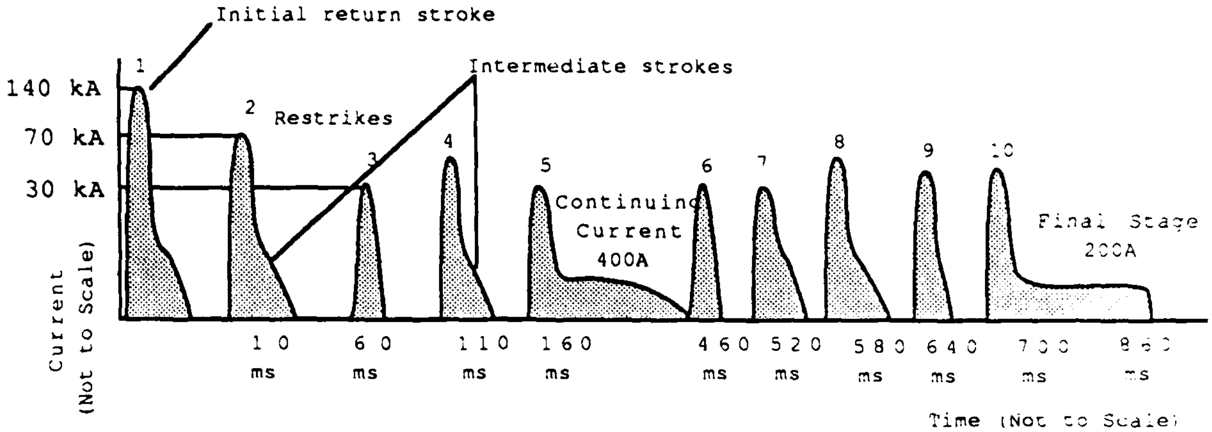
Lightning environments have varying intensities and durations because of several different physical processes involved. The variation in parameters makes it impossible to specify the environment during any particular lightning flash. Lightning occurs most frequently due to charge separation in thunderstorm clouds. During a storm, air convection currents cause charge centers to build up within clouds. Because of mutual capacitance, the potential between these charge centers increases and will eventually break down a portion of the air path between them, redistributing the charges. The number of strokes within each flash and the peak currents depend on many factors including the storm intensity, the charge levels in the cloud before the leader has completed a path to the opposite charge, and the cloud base height (Melander and Cooley, 1984). These factors are variable, and more than an order of magnitude difference may occur between the currents of successive strikes.

Lightning flashes are of two fundamentally different forms, cloud-to-ground and inter/intracloud. Discharges may originate from either a positive or a negative charge center in a cloud and terminate at the ground or in an opposite charge center in the cloud. A negative discharge is characterized by several intermittent strokes and continuing currents. A positive discharge occurs only a small percentage of the time. It is characterized by both higher average current and longer duration within a single stroke. (See figure 2.2-1.)

Once preliminary breakdown within a cloud has begun, the breakdown process proceeds by a stepped leader which propagates from the cloud toward the ground or towards another charge center. As a stepped leader approaches the source of opposite charge, high electrical fields are produced. These fields give rise to streamers initiated at the ground or charge center until one of these

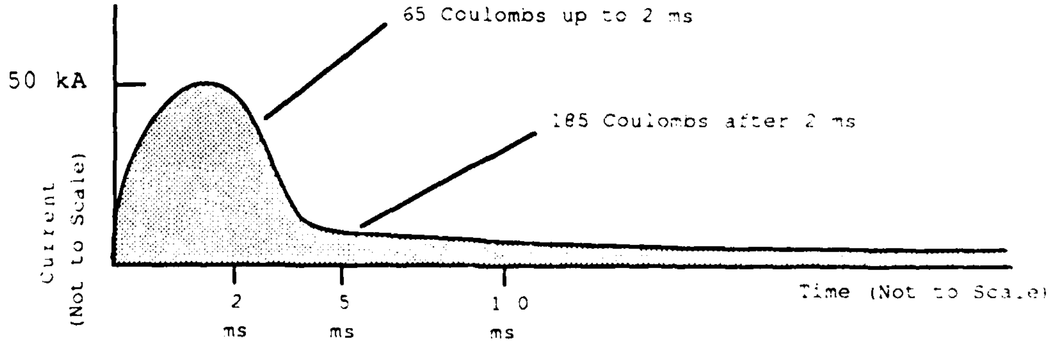
For Each Stroke:
Time to peak current = 1.5 μs
Time to half value = 40 μs

For the complete flash:
$\int i^2 \, dt = 1.9E6 \; A^2 \; s$



(A) Severe negative lightning flash current waveform.
(Courtesy of Cianos/Pierce)

For the complete flash:
$\int i^2 \, dt = 2.5E6 \; A^2 \; s$



(B) Moderate Positive Lightning Flash Current Waveform

FIGURE 2.2-1. LIGHTNING FLASH CURRENT WAVEFORM

streamers contacts the approa:hing stepped leader. The average velocity of propagation of the stepped leader is about one meter per microsecond for each step tens of meters in length and separated in time by approximately 50 $\mu$s. The typical current is 1000 amperes and the average charge in the entire stepped leader channel is about 5 coulombs.

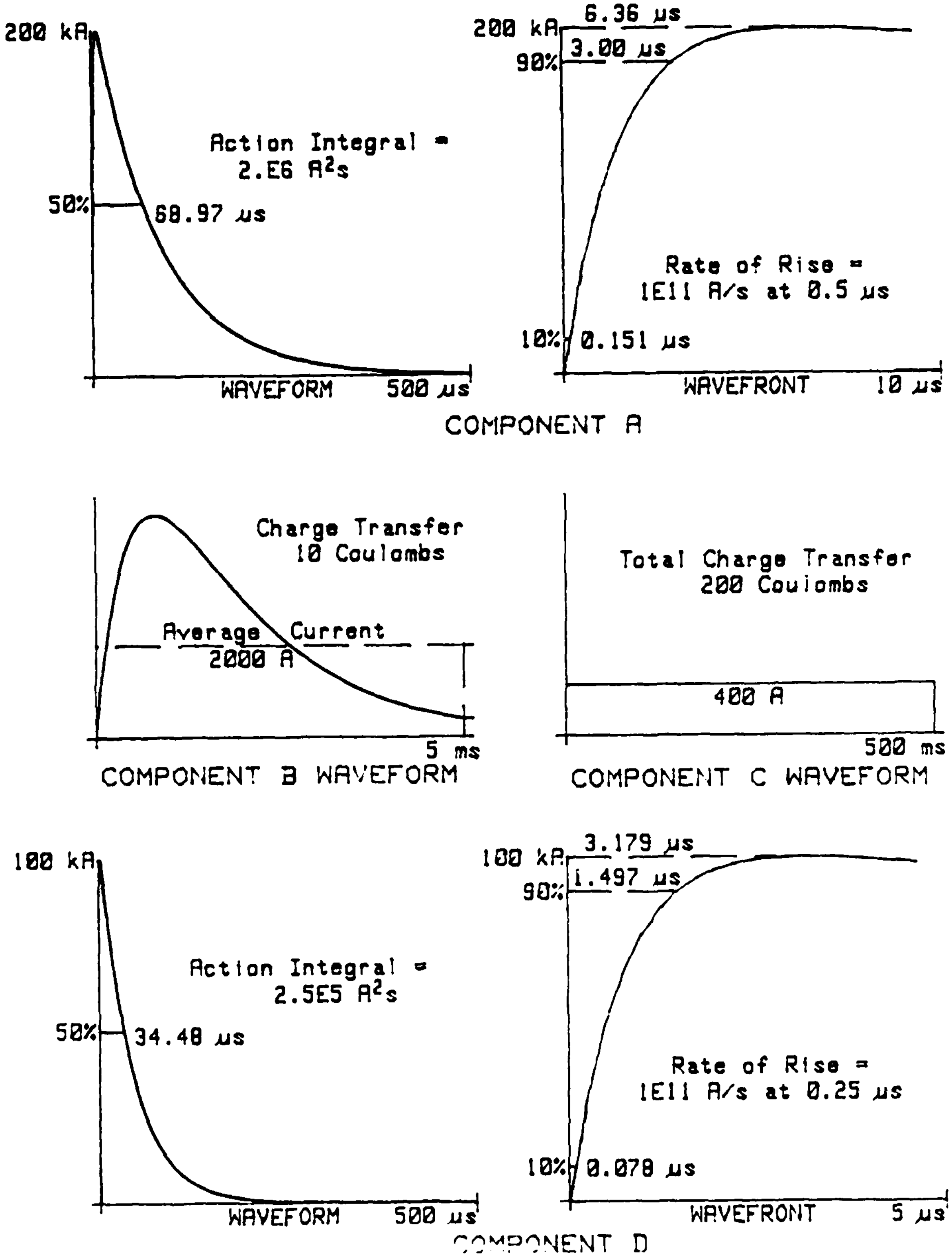
The high peak current associated with lightning occurs after the stepped leader reaches the ground and forms the return stroke of the lightning flash. This return stroke occurs when the charge in the leader channel is suddenly able to flow into the low impedance ground. The return stroke current expected value is much larger than the leader current and ranges between 10 and 30 kA. Although in rare cases a larger current can occur, a peak current of 200 kA represents a severe stroke and is considered a practical maximum value of lightning current. In rare cases, a larger current can occur. The current in the return stroke has a fast rate of change, ranging between 10 and 20 kA/$\mu$s. The maximum practical value is considered to be 200 kA/$\mu$s. No correlation has been shown to exist between peak current and peak rate of rise. The return stroke may be followed by a dart leader which initiates one or more subsequent return strokes or restrikes. Restrikes will continue until the charge is neutralized. Subsequent strokes typically have smaller magnitudes and faster rise times but comparable rates of change to the first return stroke. A lightning flash may contain as many as 24 restrikes following the first return stroke. Restrikes occur at intervals of several tens of milliseconds as different charge centers in the cloud are tapped.

The total charge transported by the lightning return stroke is relatively small, a few coulombs. Most of the charge is transported as a continuing current. Currents on the order of a few hundred amperes may flow in the ionized channel for periods up to one second. The maximum charge transferred is 200 coulombs. Continuing currents may link successive return strokes.

A discharge between clouds or charge centers within a cloud is characterized by a multitude of relatively low level intermittent strokes and continuing currents. The average velocity of propagation of the streamers is $10^5$ meters per second. The peak current associated with an inter/intracloud discharge is in the range of 3 to 10 kA and occurs when opposite charge centers have been connected by a streamer or stepped leader. Each restrike within an inter/intracloud lightning flash may contain 20 separate pulses, known as a multiple burst. The number of restrikes is comparable to a cloud-to-ground flash.

Important parameters of a lightning flash are the peak current amplitude, maximum current rate-of-rise, energy, duration, rise-time, and the number of strokes within each flash. Statistical representations of these measured parameters are found in Melander and Cooley (1984). The great bulk of this statistical data is based on measurements of cloud-to-ground flashes. Several flight test programs within the past few years have gathered data on inter/intracloud lightning. These data are used to define parameters for lightning threat levels.

Representations of the various portions of lightning flashes have been developed by the Society of Automotive Engineers (SAE) committee AE4L as shown in figure 2.2-2. Multiple stroke and multiple burst waveforms are characterized



COMPONENT A

COMPONENT B WAVEFORM

COMPONENT C WAVEFORM

COMPONENT D

FIGURE 2.2-2. IDEALIZED LIGHTNING CURRENT WAVEFORMS

in figure 2.2-3. Table 2.2-1 summarizes the parameters for each waveform. A double exponential of the form shown below defines each component waveform.

$$I(t) = I_0 \, x \, (e^{-\alpha t} - e^{-\beta t})$$

## 2.3. Interaction and Coupling to Aircraft

It is not possible to precisely quantify the lightning environment during any particular strike to an aircraft in flight. At low altitudes, cloud-to-ground strikes are more likely. Inter/intracloud strikes are more common at higher altitudes. Statistics on the number of strikes to aircraft as a function of altitude are given in figure 2.3-1.

It is generally accepted that the presence of an aircraft may trigger the leader discharge process between charge centers by disrupting the leader path. Recent experience by the FAA and the Air Force Wright Aeronautical Laboratory (AFWAL) in-flight program using a CV-580 to intercept lightning strikes indicates leader growth out of the wing of the test aircraft. Figure 2.3-2 illustrates the interaction of the aircraft with a charge center. When the aircraft is part of a leader not much current flows. The major effect occurs when the path is complete to the opposite charge center, and the return current passes through the aircraft.

A typical lightning flash consists of 20-200 current pulses over a one to two second interval. Because the aircraft is moving, the flash will sweep aft from an initial attachment point, all the while reattaching to spots along the line of flight aft from the original point of attachment. A portion of the current will enter the aircraft at several points along the path from the initial and swept attachment points. Figure 2.3-3 shows a typical path of attachment points for a swept flash. If the attachment is a trailing edge surface, then the current will hang on at this initial point and flow through there for the entire flash.

### 2.3.1. Standard Aircraft Lightning Environment

Since different parts of an aircraft must tolerate different levels of current, a standard definition has evolved defining the levels of current applicable to different zones of the aircraft. The SAE-AE4L committee has established generally accepted definitions of the possible strike zones as follows:

- Zone 1A: Initial Attachment Point with low probability of flash hang on, such as a leading edge.
- Zone 1B: Initial attachment point with high probability of flash hang-on, such as a trailing edge.
- Zone 2A: A swept stroke zone with a low probability of flash hang-on, such as a wing midspan.
- Zone 2B: A swept stroke zone with high probability of flash hang-on, such as the wing inboard trailing edge.

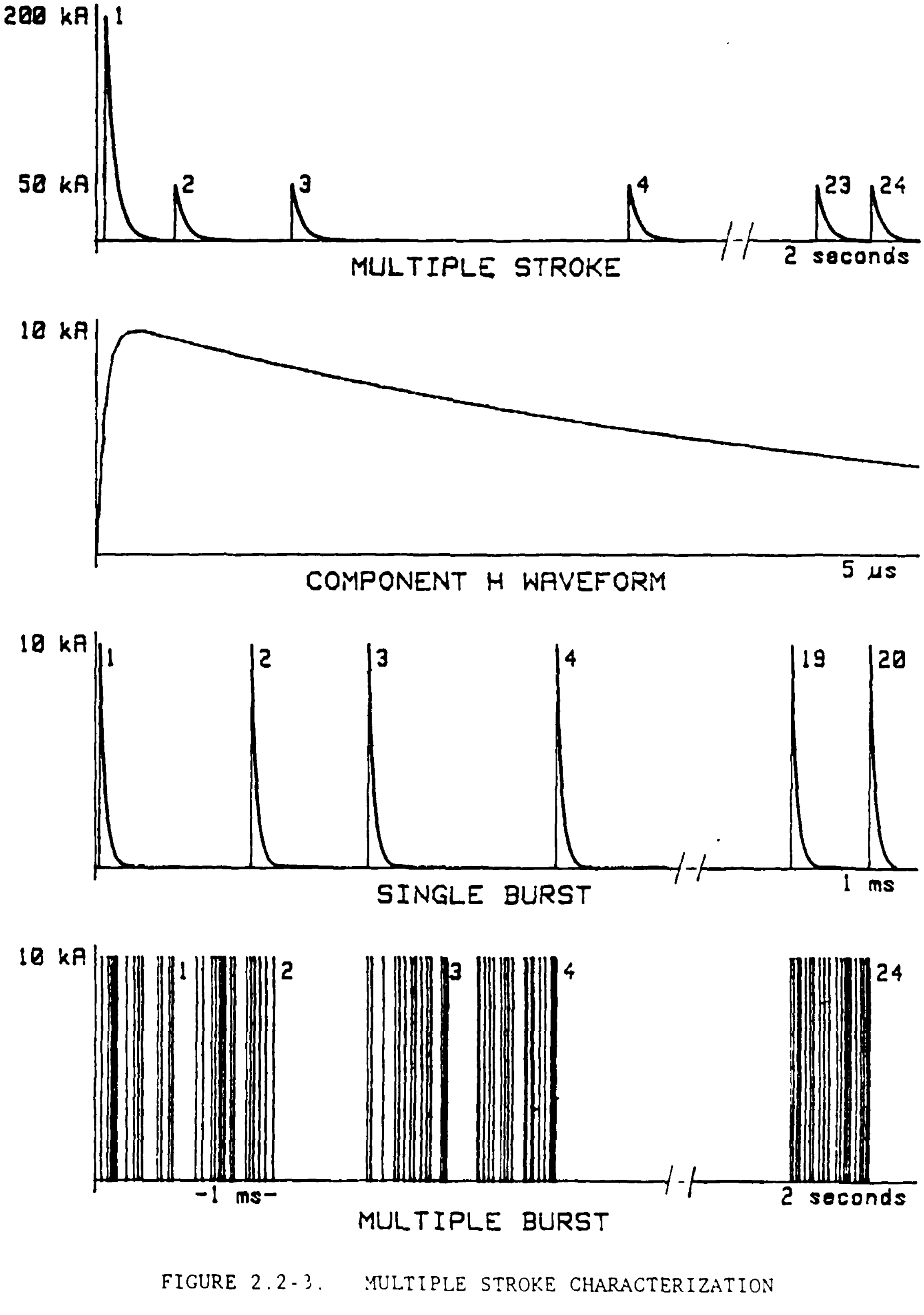


FIGURE 2.2-3. MULTIPLE STROKE CHARACTERIZATION

TABLE 2.2-1. IDEALIZED LIGHTNING WAVEFORM PARAMETERS

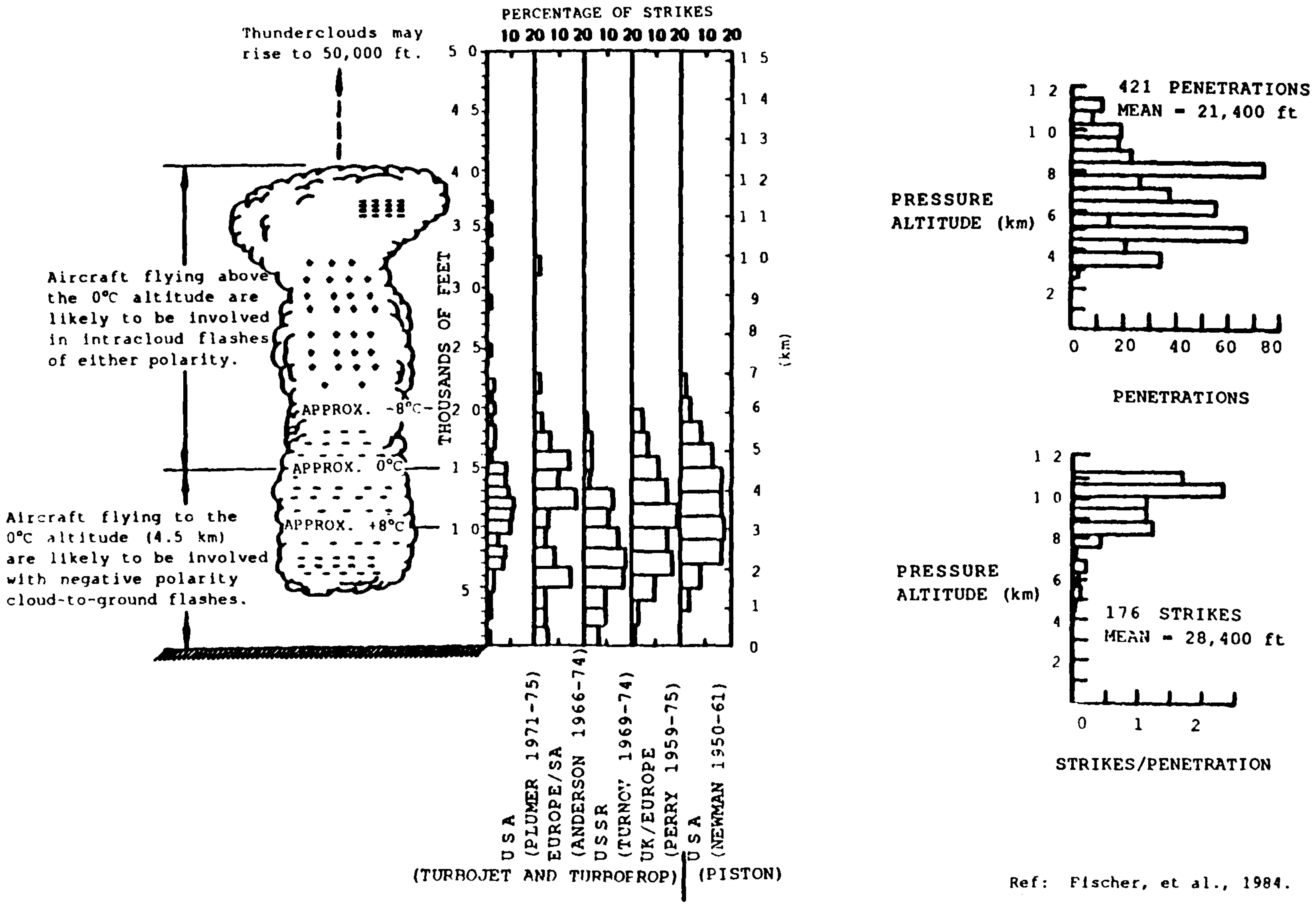
| Threat | $I_o$ (A) | Alpha (1/s) | Beta (1/s) | Peak Current (kA) | Maximum Rate-of-Rise (kA/$\mu$s) | Action Integral ($A^2$s) |
|---|---|---|---|---|---|---|
| Severe Component A[1,2,3] | 218810 | 11354 | 647265 | 200 | 140 | $2.0\times10^6$ |
| Intermediate Current Component B[2] | 11300 | 700 | 2000 | 4.2 | NA | NA |
| Continuing Current Component C | 400 | | | 0.4 | | |
| Restrike Component D[2,4] | 109405 | 22708 | 1294530 | 100 | 140 | $2.5\times10^5$ |
| Multiple Stroke Component D/2[2] | 54703 | 22708 | 1294530 | 50 | 70 | $6.2\times10^4$ |
| Multiple Burst Component H[2] | 10572 | 187191 | 19105100 | 10 | 200 | NA |

[1] This component represents a very severe stroke, exceeding approximately 99.5 percent of all recorded strokes.

[2] The double exponential form is convenient for low level tests and analytical procedures.

[3] Rate of rise represents 90 to 95 percent severity level.

[4] Rate of rise is the same as that of Component A to recognize the fact that recorded rise times of subsequent strokes are often as short or shorter than those of the first return stroke.



Ref: Fischer & Plumer, 1977.

Ref: Fischer, et al., 1984.

FIGURE 2.3.1. AIRCRAFT LIGHTNING STRIKE INCIDENTS AS A FUNCTION OF ALTITUDE

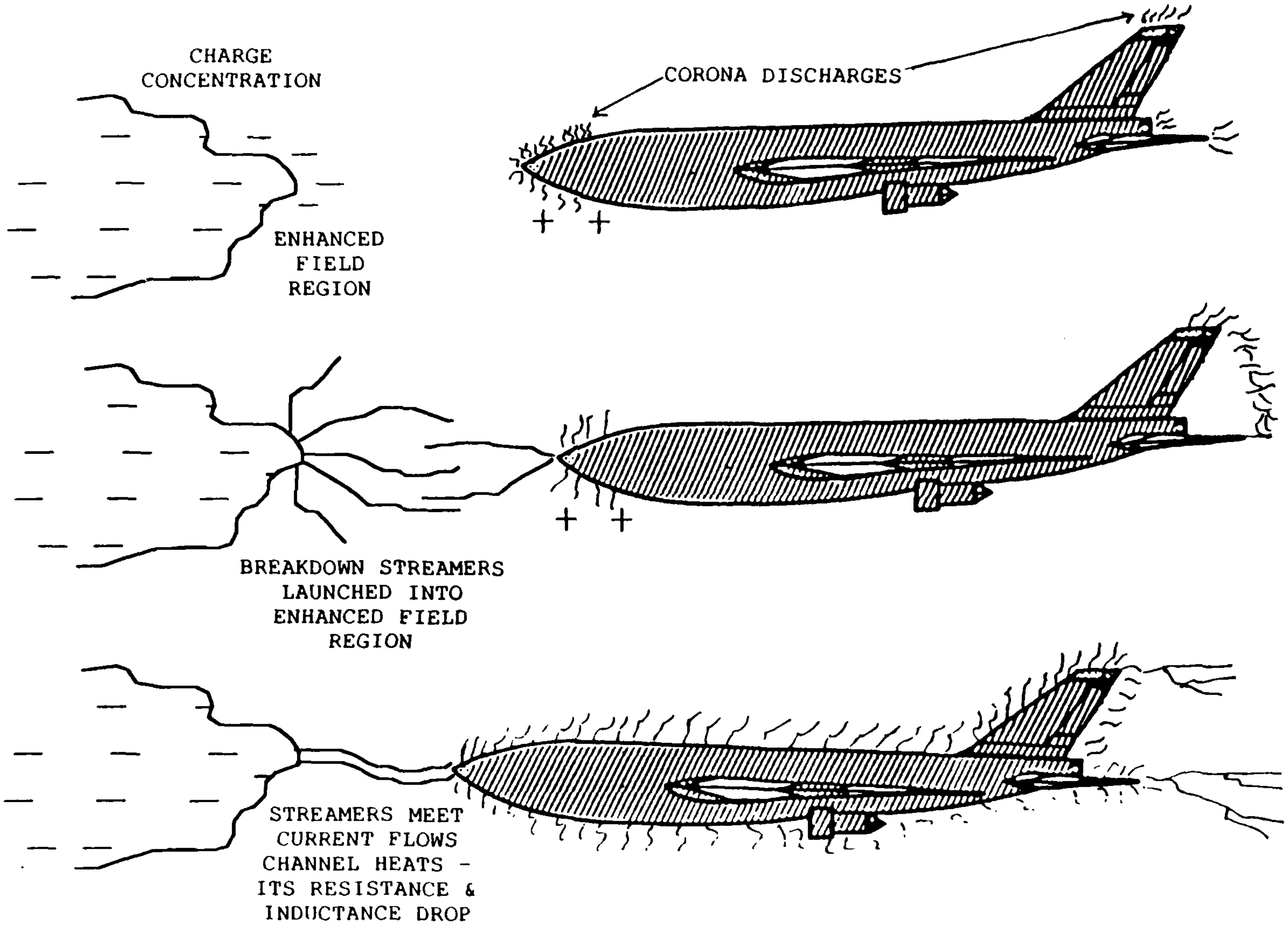

CHARGE CONCENTRATION
CORONA DISCHARGES
ENHANCED FIELD REGION
+ +
BREAKDOWN STREAMERS LAUNCHED INTO ENHANCED FIELD REGION
+ +
STREAMERS MEET CURRENT FLOWS CHANNEL HEATS - ITS RESISTANCE & INDUCTANCE DROP

FIGURE 2.3-2. INTERACTION OF AIRCRAFT WITH CHARGE CENTERS

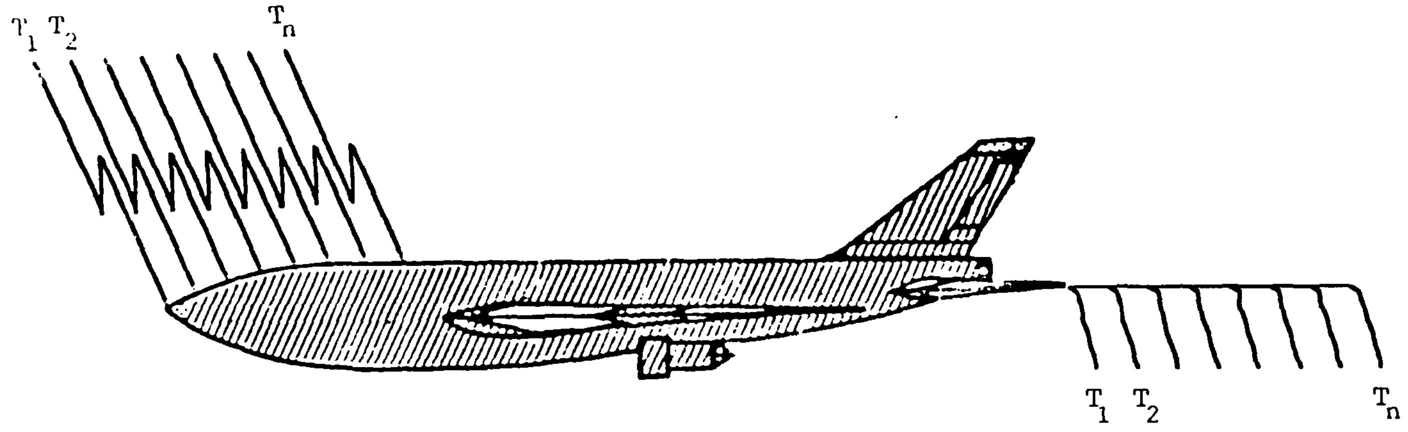


FIGURE 2 [illegible]-3. TYPICAL PATH OF SWEPT FLASH ATTACHMENT POINTS

- Zone 3: The remainder of the vehicle that is not covered by Zone 1 and Zone 2. There is a low probability of any attachment of the direct lightning flash arc. Zone 3 areas may carry large amounts of electric current, but only as a result of conduction between pairs of direct or swept stroke attachment points.

The SAE-AE4L committee has established the current levels to be expected in each of the strike zones to be used for test or certification purposes. An idealized representation of these defined current components for a complete flash is shown in figures 2.3-4 and 2.3-5.

The location of strike zones is well established for current aircraft configurations, see figures 2.3-6 and 2.3-7, but if configurations differ much from today's aircraft, locating the lightning strike zones may require careful interpretation of the particular geometry to determine the location and extent of the areas where lightning may attach, sweep, and hang-on.

A tabulation of lightning strike statistics is given in table 2.3-1 for major sections of commercial aircraft. In this grouping, the four sections most often struck by lightning are the nose, fuselage, wing, and horizontal stabilizer. The wide body jets also had high strike rates to antennas.

### 2.3.2. Structural Materials Effect on Strike Zones

A study by Grumman Aircraft Company investigated the strike attachment zones for an advanced fighter configuration (Craft, 1981). A scale model of the aircraft with replaceable panels for portions of the skin was used. The panels were made from aluminum, G/E, and kevlar. The study concluded that there is no essential difference between the strike zones for panels of G/E and aluminum. However, there is considerable difference for kevlar panels. Kevlar is a non-conductor; therefore, a lightning arc will jump over or along the surface rather than attach to kevlar.

Other studies have shown that the lightning arc will punch through kevlar to reach metal portions under the kevlar skin panels. This is also reported to be the case for radomes used to cover nose-mounted radar equipment. Lightning will readily puncture a radome to reach metallic portions of an all-metal aircraft. These items are described in a report by Fisher and Plumer.

## 2.4. Lightning Effects on Aircraft Systems

### 2.4.1. Range of Lightning Effects

Direct effects result from direct action of the lightning arc in the form of arcing and sparking on the aircraft; therefore, the term "direct effects." Evidence of this is seen as gross damage from the action of the arc on the materials. Protection against direct effects must come from the structure or protective diverters which prevent the currents from flowing into the sensitive areas. Important lightning parameters, which determine damage due to direct effects, are the dwell time on the aircraft, the peak current, the duration of

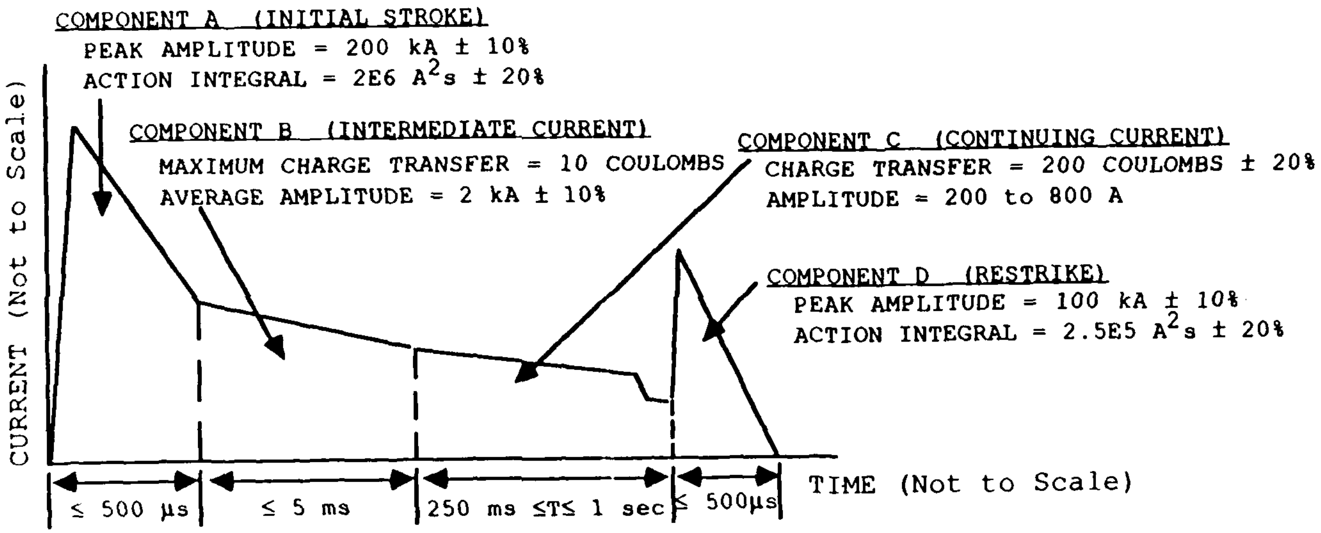

COMPONENT A (INITIAL STROKE)
PEAK AMPLITUDE = 200 kA ± 10%
ACTION INTEGRAL = 2E6 A²s ± 20%
COMPONENT B (INTERMEDIATE CURRENT)
MAXIMUM CHARGE TRANSFER = 10 COULOMBS
AVERAGE AMPLITUDE = 2 kA ± 10%
COMPONENT C (CONTINUING CURRENT)
CHARGE TRANSFER = 200 COULOMBS ± 20%
AMPLITUDE = 200 to 800 A
COMPONENT D (RESTRIKE)
PEAK AMPLITUDE = 100 kA ± 10%
ACTION INTEGRAL = 2.5E5 A²s ± 20%
CURRENT (Not to Scale)
TIME (Not to Scale)
≤ 500 µs
≤ 5 ms
250 ms ≤T≤ 1 sec
≤ 500µs

FIGURE 2.3-4. LIGHTNING CURRENT COMPONENTS EXPECTED IN EACH ZONE

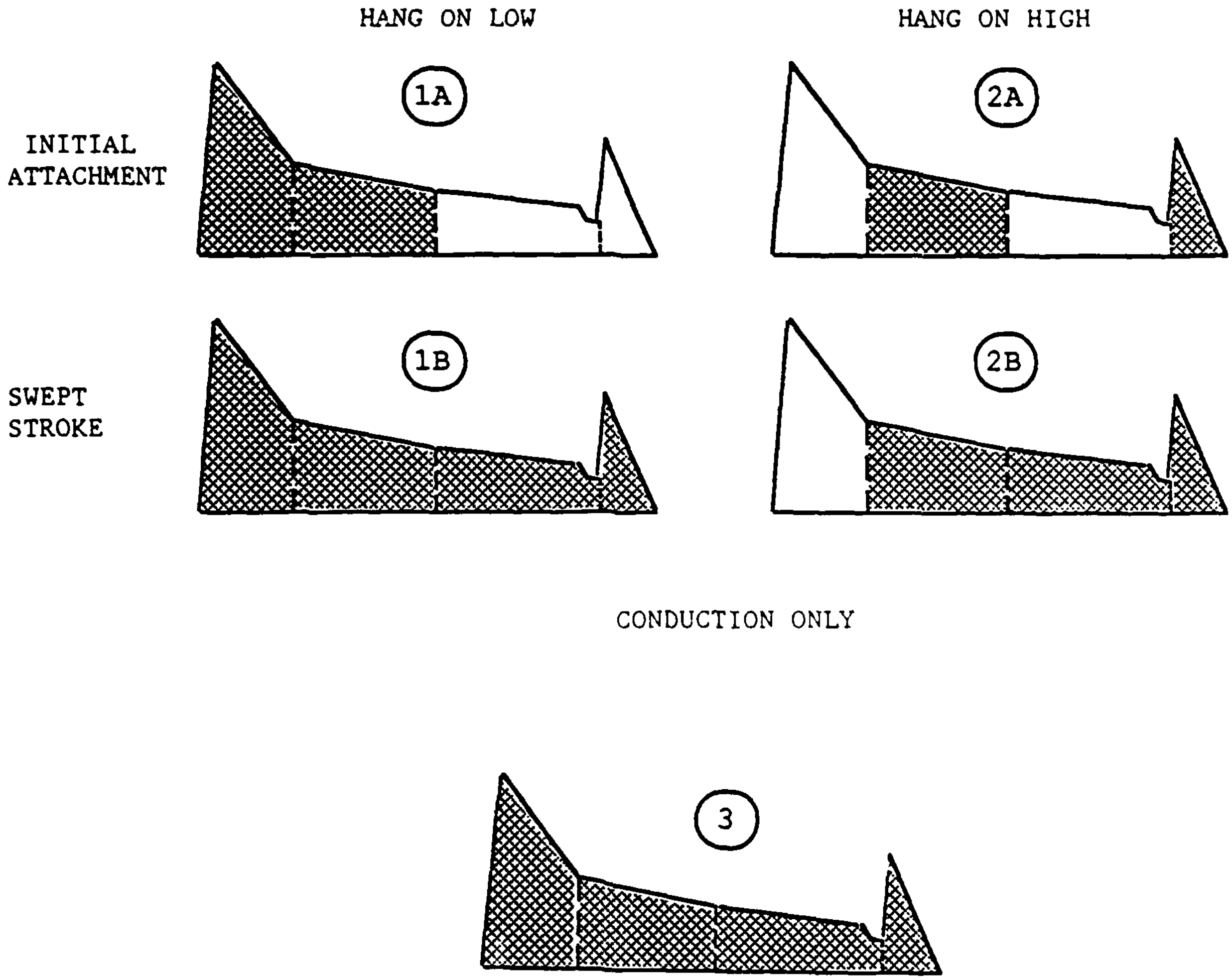
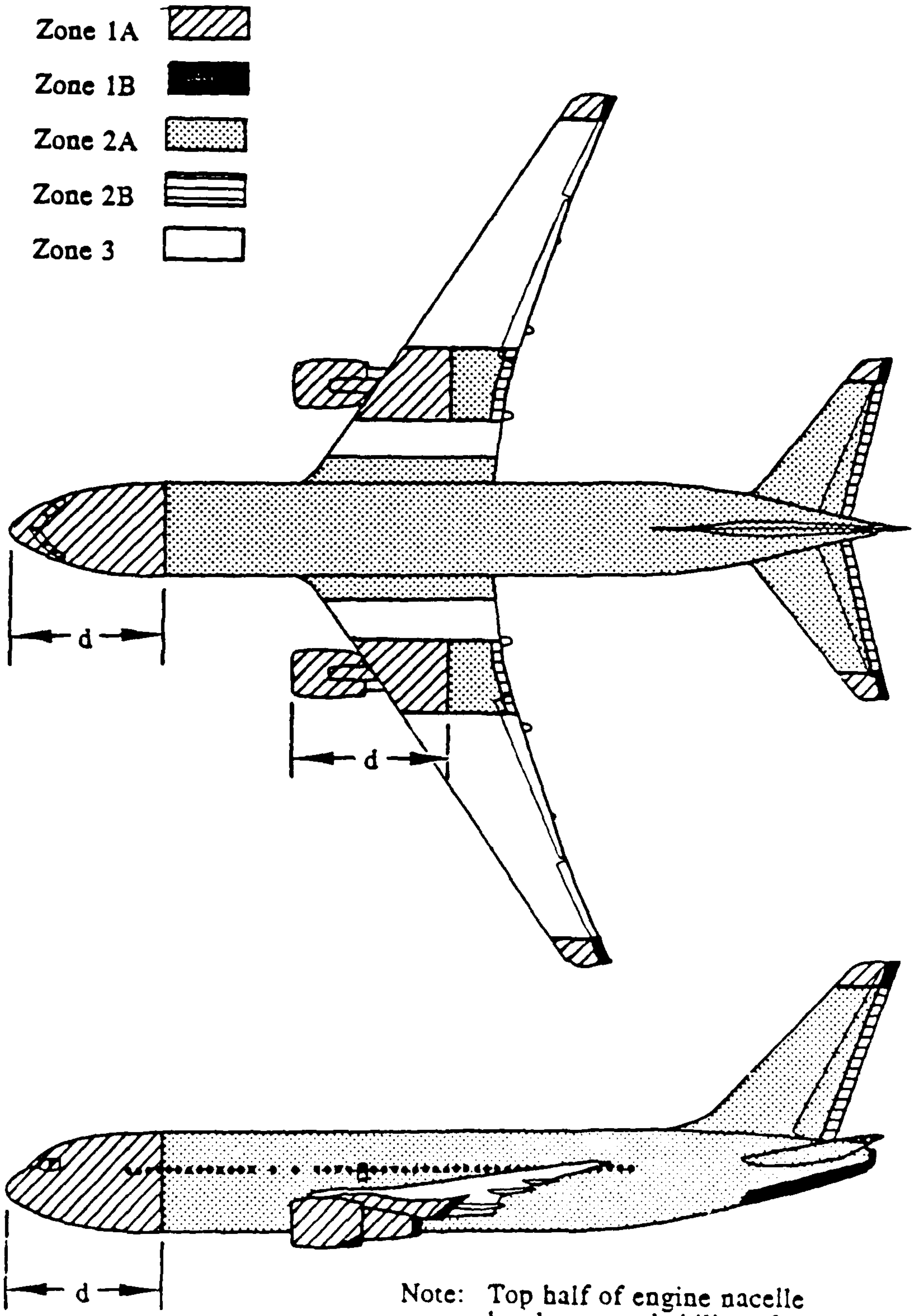


FIGURE 2.3-5. LIGHTNING CURRENT COMPONENTS EXPECTED IN EACH ZONE



Note: Top half of engine nacelle has lower probability of any strike than bottom.

FIGURE [illegible] TYPICAL LIGHTNING STRIKE ZONES

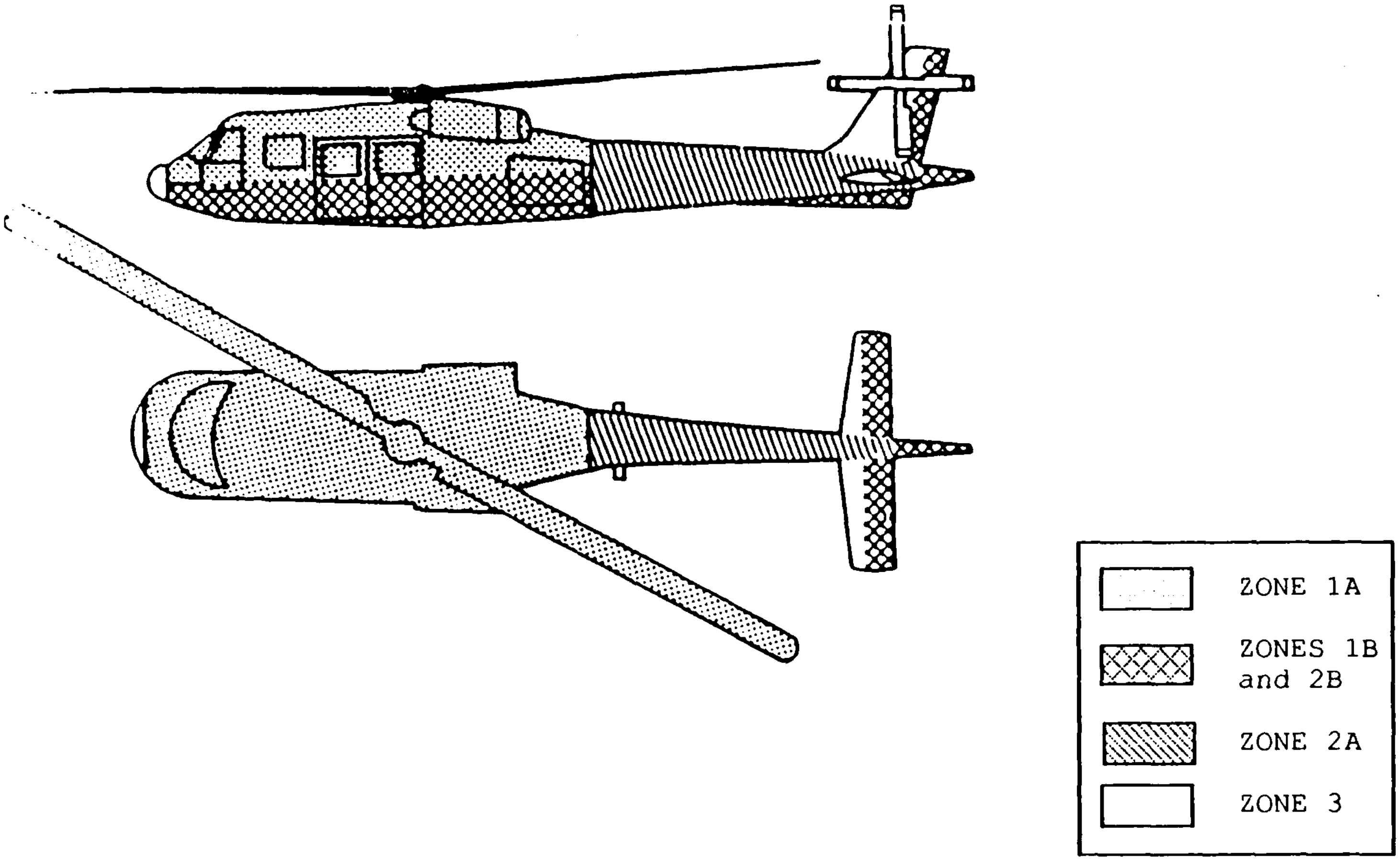


FIGURE 2.3-7. TYPICAL LIGHTNING STRIKE ZONES FOR HELICOPTERS
(User's Manual for AC-20-53, 1987)

TABLE 2.3-1. COMMERCIAL AIRPLANE LIGHTNING STRIKE STATISTICS

| | JET<br>2 ENGINE<br>AFT MOUNTED<br>T-TAIL | | JET<br>3 ENGINE<br>AFT MOUNTED | | JET<br>4 ENGINE<br>WING MOUNTED | | JET<br>TOTAL<br>NARROW BODY | | JET<br>WIDE BODY | |
|---|---|---|---|---|---|---|---|---|---|---|
| | NO. | % | NO. | % | NO. | % | NO. | % | NO. | % |
| NOSE | 3 | 19 | 29 | 30 | 83 | 43 | 115 | 38 | 220 | 34 |
| WING | - | - | 24 | 24 | 33 | 17 | 57 | 19 | 99 | 15 |
| HORIZONTAL STABILIZER | 6 | 38 | 6 | 6 | 24 | 13 | 36 | 12 | 59* | 9* |
| VERTICAL STABILIZER | - | - | 14 | 14 | 12 | 6 | 26 | 8 | | |
| FUSELAGE | 5 | 31 | 20 | 20 | 38 | 20 | 63 | 21 | 112 | 17 |
| ANTENNAS | 2 | 13 | 1 | 1 | 2 | 1 | 5 | 2 | 100 | 15 |
| ENGINE | - | - | 1 | 1 | - | - | 1 | < 1 | 24 | 4 |
| TAIL | - | - | 3 | 3 | - | - | 3 | 1 | 35 | 5 |
| TOTAL | 16 | | 98 | | 192 | | 306 | | 649 | |

Ref: Cooley, Geren, and Melander; Sept. 1982

* HORIZONTAL/VERTICAL COMBINED

current, the maximum current rate-of-rise, and the number of restrikes. Aircraft parameters, which deteremine damage due to direct effects, are skin type, skin thickness, and paint.

Damage may also occur from indirect effects that damage components or disrupt the software operations of electrical and electronic systems. Indirect effects are generally more subtle than direct effects, because the physical damage from indirect effects is not easily seen. Indirect effects are caused by the transient voltages and currents that are induced into the wiring as a result of the lightning arc and the associated EM fields on the aircraft structure. Important parameters are the peak current, maximum current rate-of-rise, maximum EM fields rate-of-rise, number of restrikes, and for non-metal aircraft the duration of current flow.

Protection design for lightning indirect effects has many factors. Parameters to be considered when protection beyond the baseline configuration is needed include protection provided by the structure, cost, weight, reliability, impact on vehicle performance, expected life cycle, and protection necessary against other EM threats.

Table 2.4-1 lists possible effects from direct or nearby lightning strikes to aircraft in flight.

### 2.4.2. Direct Effects on Non-Metallic Structures

The most important direct effect of lightning strikes is the possible arcing and sparking in fuel areas. Other important direct effects include pitting and burning in structural materials.

For reasons discussed in Cooley (1985), direct effects protection design requires more test and analysis for composite materials than for metallic materials. For example, it is usually assumed, in the design of lightning protection, that if an electrically conductive fastener is located in an attachment zone having a high probability of hang-on, lightning will attach to the fastener. Because of the currents in the strike zone definitions, the direct attachment to a fastener in zone 1A, 1B, or 2B represents a severe worst case for any lightning strike. Although direct attachment is not a severe problem in aluminum structures, it is presently not possible to develop a fastener capable of joining advanced composite materials and carrying the full lightning current without seriously weakening the fastener. Current composite aircraft designs depend upon not having fasteners in critical parts of zone 1 and 2. Where fasteners are used, a repair procedure may be necessary for lightning strike damage.

Painted metal surfaces have longer hang-on times for swept strokes than do unpainted metal surfaces. These longer dwell times will cause deeper burning, and additional metal is required for painted metal skins on wet-wing aircraft.

Composite materials have various resin binders that burn and affect the dwell time for swept strokes. Therefore, the thickness of composite materials required for structural integrity protection against lightning strikes will

TABLE 2.4-1. RANGE OF EFFECTS FROM ATMOSPHERIC ELECTRICITY INTERACTIONS WITH AIRCRAFT

| EFFECT | CAUSE | CRITICALITY |
|---|---|---|
| Flight Control Disruption | Flight control systems have low tolerance to electrical transients caused by indirect lightning or static electrification effects. Transients may simultaneously affect parallel redundant systems. | Minor to Catastrophic |
| Fuel Tank Fire or Failure | Fuel vapor ignition may be caused by static electricity or lightning direct effects on structure. Fuel gauging and flow management electrical/electronics may spark from indirect effects. | Minor to Catastrophic |
| Loss of Engine Power | Power loss can result from possible direct effects which cause thermal or acoustic shock at engine inlet, or indirect effects of electrical transients on engine controls. | Minor to Catastrophic |
| Radome, Canopy, & Windshield Damage | Damage can occur due to direct effects of lightning strikes and arc discharge may be caused by static electricity buildup. | Minor to Catastrophic |
| Instrumentation Problems - Communications, Navigation & Landing System Interference | Instrumentation systems are disrupted by indirect transient effects caused by static electricity buildup and nearby or attached lightning strikes. | Minor to Catastrophic |
| Structural Damage | Structure damage is a result of burns or arcing and sparking from direct effects of lightning attachment to aircraft. | Minor to Catastrophic |
| Physiological Effects on Crew | Flash blindness & distracting electrical shock may be caused by the direct effects of nearby or attached lightning strikes. | Minor to Catastrophic |
| Unscheduled Deployment of Landing Gear or Control Surfaces | Premature activation of actuators is caused by indirect effects of lightning or static electricity buildup in electrical/ electronic systems. | Serious to Catastrophic |

depend upon the material's makeup as well as the fibers. It is expected that different materials of the same physical strength will behave differently when struck by lightning.

2.4.3. Indirect Effects on Non-Metallic Structures

The most important adverse feature of graphite and metal matrix materials is their lower conductivity. The conductivity factor, compared with aluminum, is 10 times less for metal matrix and 1000 times less for G/E. Lower conductivity means higher voltage drops in these structures than for a metal structure. Thus the voltage drop in a length of structure will be increased for the same level of lightning current. Because of the higher voltage drop, higher levels of currents will flow in any metallic paths such as plumbing and wiring inside an aircraft structure made from non-metallic materials. Additionally, any external EM fields will be attenuated less by a composite structure. For direct and nearby strikes, the internal EM fields will be at higher levels than for an aluminum aircraft. The exact difference in internal EM fields depends on the number of joints and openings, thickness of material, frequency range of the external EM fields, and the shape of the structure. The Atmospheric Electricity Hazards Protection (AEHP) program studies on an advanced composite (G/E) structure F-16 fuselage showed that the shielding was 15 dB for lightning pulses. It is estimated that a similar aluminum structure would have provided 30 to 40 dB of shielding, the limitation being primarily due to the number and size of openings.

In structures made from non-conductors such as kevlar and fiberglass, there is no EM shielding. This is also true for materials having very few conducting wires embedded into a non-conducting material such as Thorstrand kevlar. These materials can provide some protection against direct effects. There will be little or no improvement against indirect effects, because the magnetic shielding effectiveness of low loss factor metals, such as aluminum, is primarily due to currents flowing in the material. These currents generate EM fields which tend to cancel the incident fields. Electric field shielding is primarily due to an equipotential plane established by high conductivity metals. There are too few wires and too little metal in a material like Thorstrand to provide an effective shield against EM fields from nearby lightning sources or RF sources, such as airport radio and radar transmitters.

2.4.4. Effects on Aircraft Systems

Six examples of onboard system functions affected as a result of lightning and static electrification of aircraft are described below.

- The failure of engine instruments was experienced, as a result of lightning strikes, on an equipment version installed on a jet transport aircraft early in the development phase. The N1 tachometer and N2 were occasionally affected during lightning strikes. Electronic components in the engine tachometer transmitter were damaged. These components were connected to unshielded twisted pairs in a bundle of engine related wiring. The situation was repeated in laboratory tests and.traced to the need for 10 dB additional shielding for the wiring. The solution to this problem was to add the necessary shielding by applying aluminum foil to the upper half of the inside surface of the kevlar leading edge. This solution resulted in lighter weight than shielding the wiring.

- Possible sparks between fuel tank wiring and mechanical structures are a serious concern. For example, fuel plumbing can carry substantial currents in the event of a strike to the overflow vent tube. The fittings and plumbing must be capable of carrying these currents without sparking. Fuel gauge electrical wiring must be protected from currents on the structure path between lightning attachment and exit points along the leading and trailing edge. Currents from the cable shield to structure must not spark within the fuel tank or the fuel gauge.

- The pitot boom is often the point of attachment for lightning because of its shape and location near the front of an aircraft. The very high currents near the initial attachment can burn out the pitot heater and possibly damage electronic equipment inside the aircraft. This is particularly severe for pitot booms on aircraft with nose radomes.

- Hydraulic plumbing for flight control actuators needs to be grounded and bonded to the structure to remove high currents from the tubing fittings. These fittings have been damaged by the currents flowing in the structure and tubing from lightning strikes to the empennage. Damage was evidenced by loss of fluid in hydraulic systems.

- Static electricity results from triboelectric charging under normal flight conditions, from vehicle charging caused by nearby leaders, or as part of the initial attachment phase. High electric field breakdown discharges the accumulated charge in a repeated cycle that results in a series of sparkovers and therefore a repeating transient pulse. The electrical waveforms have wide band energy up to and including the Very High Frequency (VHF) band. Effects of static discharges appear as excessive radio noise and loss of sensitivity in the navigation and radio systems. The high electric fields have the potential to damage windscreens and damage electronic components in the window heater control.

- Lightning induced transient currents in electrical cables can cause errors in the digital data. Errors in digital bit streams are characterized by single bits or a burst of errors depending upon the baud rates. These errors are no different than those that should be expected due to other common EMI sources such as power transients, power faults, and RF and radar transmitter modulation frequencies. Digital systems designers need to consider possible disruptions in data streams similar to those that occur during long distance transmission over noisy lines and to include error detection and correction for flight critical data transmissions.

  In addition to bit stream errors, errors in digital data can occur in the discrete data signals. Discrete data input signals can be modified from true, "1", to false, "0", by transient currents, as for example, in the sensing of flaps up, wheels down, or other aircraft configuration sensors which operate as a high/low switch position. Discrete signals should not be directly used by onboard digital systems without some checks for reasonableness or low pass filtering or both. Mode change commands should be verified over five to ten samples. Discrete data outputs to indicators and actuators may also be subject to upset or damage. Faulty indicators increase crew workload and may contribute wrong information leading to hazardous flight conditions. Errors in these discrete signals are serious because they lead to wrong information regarding the aircraft configuration. Early raising of the flaps on takeoff or lowering the landing gear at cruise altitude are two obvious examples.

# 3. INDIRECT EFFFCTS PROTECTION - DESIGN APPROACH

Lightning protection for aircraft should be addressed during the design phase of the vehicle. This allows optimization of the lightning protection design and possible integration with protection designs for other EM threats. A design margin provides the definition of protection needed. This section discusses design considerations for grounding and bonding, installation of equipment, and routing of cables.

## 3.1. Design Margin

Adequate protection of equipment or systems is defined by a design margin. The design margin represents the difference between the transients induced at the interface level (by a worst case lightning strike) and the transients that the equipment is designed to withstand. This should be a positive number. A negative design margin indicates that some redesign is necessary. The size of the design margin is inversely proportional to the confidence which is given to the tests and/or analysis results used for verification.

The first step in defining a margin is to determine a threshold where the equipment becomes damaged so that it can no longer perform its intended function. Both analytical and experimental techniques are available for assessing the damage threshold. The techniques might be used during equipment design where the thresholds are specified, or during overall vehicle assessment where thresholds are used to establish Equipment Transient Design Levels (ETDL).

The equipment transient susceptibility level is another name for the damage threshold. This level will normally be somewhat higher than the ETDL, which represents the amplitude of voltage and/or current that the equipment is required to withstand or tolerate and remain operational. The ETDL, in turn, will be set higher than the maximum amplitude of transients that are allowed to occur on interconnecting wiring, the Transient Control Level (TCL). The relationship between transient control, equipment transient design, and susceptibility levels is illustrated in figure 3.1-1.

Standardized definitions of induced voltage and current waveforms and amplitudes that are representative of transients which appear in interconnecting wiring are found in AC 20-53. ETDLs may be selected from among the amplitude levels presented; TCLs can be derived by providing an adequate margin. Normally the transient control and design levels will be established by the airframe manufacturer or system integrator, who will compare the penalties of vehicle or interconnecting wiring protection with those of equipment hardening to establish the most efficient levels.

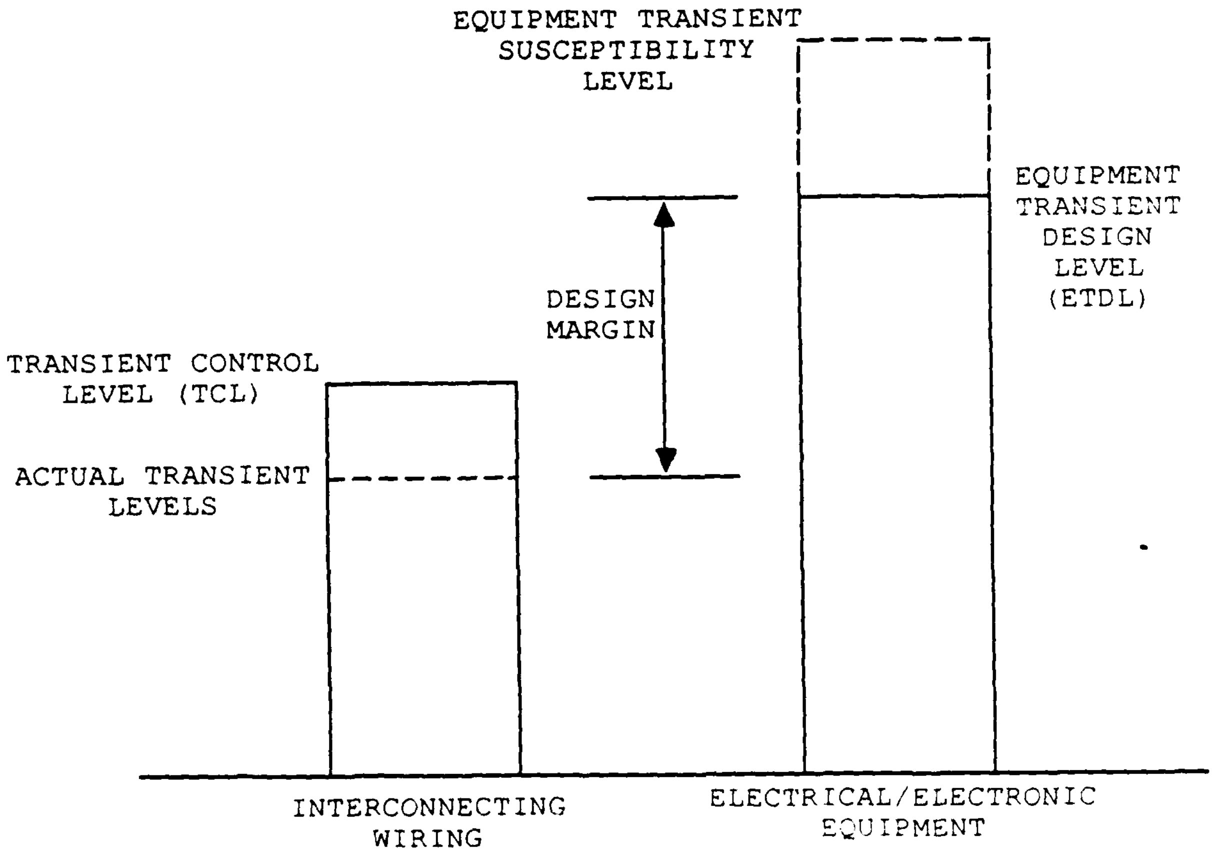

EQUIPMENT TRANSIENT SUSCEPTIBILITY LEVEL
EQUIPMENT TRANSIENT DESIGN LEVEL (ETDL)
DESIGN MARGIN
TRANSIENT CONTROL LEVEL (TCL)
ACTUAL TRANSIENT LEVELS
INTERCONNECTING WIRING
ELECTRICAL/ELECTRONIC EQUIPMENT

FIGURE 3.1-1. DESIGN MARGIN DEFINITION

### 3.2. Requirements for Grounding and Bonding

Grounding and bonding of the electronic equipment in an aircraft presently has a requirement for 2.5 milliohms from chassis to chassis (MIL-B-5087B, 1970). The resistance requirement was established early to assure that potential interference sources in different equipment would be isolated from sensitive electronics. The basis for the number chosen was one of engineering judgement. If the resistance was zero, there would be no interference or hazard to personnel due to power system faults or lightning. It is particularly convenient to use the 2.5 milliohm value for assessment of system protection against lightning. If 200,000 amps flows in a 2.5 milliohm resistor, the maximum voltage drop will be 500 volts. If every bond has less than 2.5 milliohms resistance, then no end-to-end validation testing is necessary, providing each unit of equipment will withstand 500 volts.

For the most part, aluminum and titanium alloys present no major difficulties in meeting the 2.5 milliohm specification. Maintaining adequate conductivity throughout an airframe has been a problem only when good contact between mating parts could not be maintained. Breaks in conduction paths are necessary at doors, hinges, and control surfaces. Corrosion control often requires a nonconductive coating on parts. Where interruptions in the grounding path occur, bonding requirements are met by reestablishing the conduction path using a metal jumper or strap. Utilizing present metal aircraft design approaches for composite craft will not yield the 2.5 milliohm resistance required.

Requirements for direct effects protection require that the grounding and bonding system be spark free in fuel areas, and that load bearing elements are not seriously degraded upon experiencing a lightning strike. Meeting these requirements requires an experimental approach.

Requirements for indirect effects protection of electrical/electronic systems against lightning strikes depend upon meeting the operational requirements of the equipment. The need for adequate grounding and bonding is well established by operational experience. For example, aircraft having poor grounding and bonding (i.e., poor or no electrical conduction throughout the structure and wiring) may be subject to operational hazards varying from major to minor. When different parts of the aircraft and wiring are not electrically connected, differences in potential can build up between them. Since the ultimate breakdown potential of air is lowered with altitude, corona or sparks may occur. Furthermore, fuses or circuit breakers to protect against shorts in equipment and wiring may not open properly. These factors lead to the following:

- Fuel explosion hazards from sparking in fuel gauges and wiring.
- Static discharges that may rupture windows (dielectric).
- Personnel electric shock hazards.
- Electronic equipment damage - burn out.
- Electrical/electronic systems malfunctions.

- Excessive radio noise when communicating with airport or other aircraft.

The electrical function of a bonding and grounding system for protection of electronic and electrical equipment is to provide a low impedance ground path for current flow. Table 3.2-1 indicates the current levels that may be expected from various sources.

The path impedance should be low enough that these interference sources will not produce a high voltage value that can disrupt equipment functions. Electrical/electronic equipment can be made to tolerate voltage differences of a few volts between units. Typical values for equipment tolerance against transients are shown in table 3.2-2.

Tolerable levels of ground impedance, based upon values in tables 3.2-1 and 3.2-2, are shown in table 3.2-3. This data indicates that the range of acceptable ground impedance values depends upon the source of interference and the degree of protection built into the installation and equipment. Equipment containing large scale integrated circuits can be designed and built to withstand 600 volt potential differences. This level of protection requires balanced circuits, high impedance input networks, and twisted pair wiring. More typical circuitry can withstand 10 volts between units by using balanced circuits. Single ended digital circuits can only tolerate a few volts between units for TransistorTransistor Logic (TTL) circuits that operate with 5 volt logic levels.

## 3.3. Guidelines for Cable Routing and Equipment Installation

The aircraft structure has a significant influence on the lightning protection measures needed for a specific design. The structure provides the first layer of protection from lightning. If the structure were a solid shell and a perfect conductor, no other protection measures would be necessary. In reality, there are apertures, joints, and imperfect conductors. These lead to leakage of fields and currents penetrating to the interior of the aircraft. It becomes necessary to select ways to minimize coupling to internal wiring.

Protection may be provided by increased shielding on exterior cables, good bonding at apertures, selective cable routing, surge arrestors, and wiring configuration between circuits.

Proper ways of penetrating the structure or equipment are illustrated in figure 3.3-1. These techniques maintain the protection integrity of the outer structure rather than allowing currents to penetrate the vehicle interior.

As a general rule, wiring should be routed near a good ground or reference plane and away from joints and apertures. A ground plane provides a common low impedance reference for equipment and also provides a fault return for power systems. Multiple connections between the ground plane and the structure allow division of the lightning current between the metal ground and structure. This is essential for composite structures.

TABLE 3.2-1. GROUND SYSTEM CURRENTS FROM A VARIETY OF EM SOURCES

| CURRENT SOURCE | RANGE OF CURRENT |
|---|---|
| 1. Lightning currents, broad band pulses. | 20 KA to 200 kA |
| 2. Power system fault currents, continuous wave 400 Hz. | 100 A to 1000 A |
| 3. RF current returns from on board transmitters and transponders, continuous wave HF, VHF, UHF, and microwave. | 1 A to 10 A |
| 4. Currents from nearby sources of RF energy such as radar and radio transmitters, continuous wave HF, VHF, UHF, and microwave. | 1 A to 10 A |
| 5. Power currents resulting from relays, strobe lights, and other high pulse current devices. | 5 A to 50 A |
| 6. Digital and analog signals between units of equipment, CW and Pulses 100 Hz to 10 MHz. | 10 ma to 5 A |

TABLE 3.2-2. TYPICAL INTERFERENCE TOLERANCE LEVELS BETWEEN UNITS OF ELECTRONIC EQUIPMENT

| | |
|---|---|
| 1. Lightning Pulses (a) | 600 volts |
| 2. Power System Faults (b) | 10 volts |
| 3. Continuous Waves HF Frequencies | 50 volts |
| 4. Continuous Waves VHF Frequencies | 100 volts |
| 5. Continuous Waves UHF Frequencies | 100 volts |
| 6. Tracking Radar (Sweep Frequency) | 10 volts |

NOTES: (a) Specially protected against lightning by balanced signals, high impedance, and twisted pair circuits.
(b) Circuits unprotected except balanced signals, twisted pair wiring.

TABLE 3.2-3. TOLERABLE LEVELS FOR GROUND IMPEDANCE IMPLIED BY TABLE 3.2-1 AND TABLE 3.2-2 VALUES

| | |
|---|---|
| 1. Lightning Pulses | 3 to 30 milliohms |
| 2. Power System Faults 400 Hz | 10 to 100 milliohms |
| 3. Continuous Waves HF | 5 to 50 ohms |
| 4. Continuous Waves VHF | 10 to 100 ohms |
| 5. Continuous Waves UHF | 10 to 100 ohms |
| 6. Tracking Radar (Sweep Frequency) | 0.1 to 1 ohm |
| 7. Power Currents From Onboard Pulsed Current Devices | 20 to 200 milliohms |
| 8. Digital and Analog Signals | [illegible] |

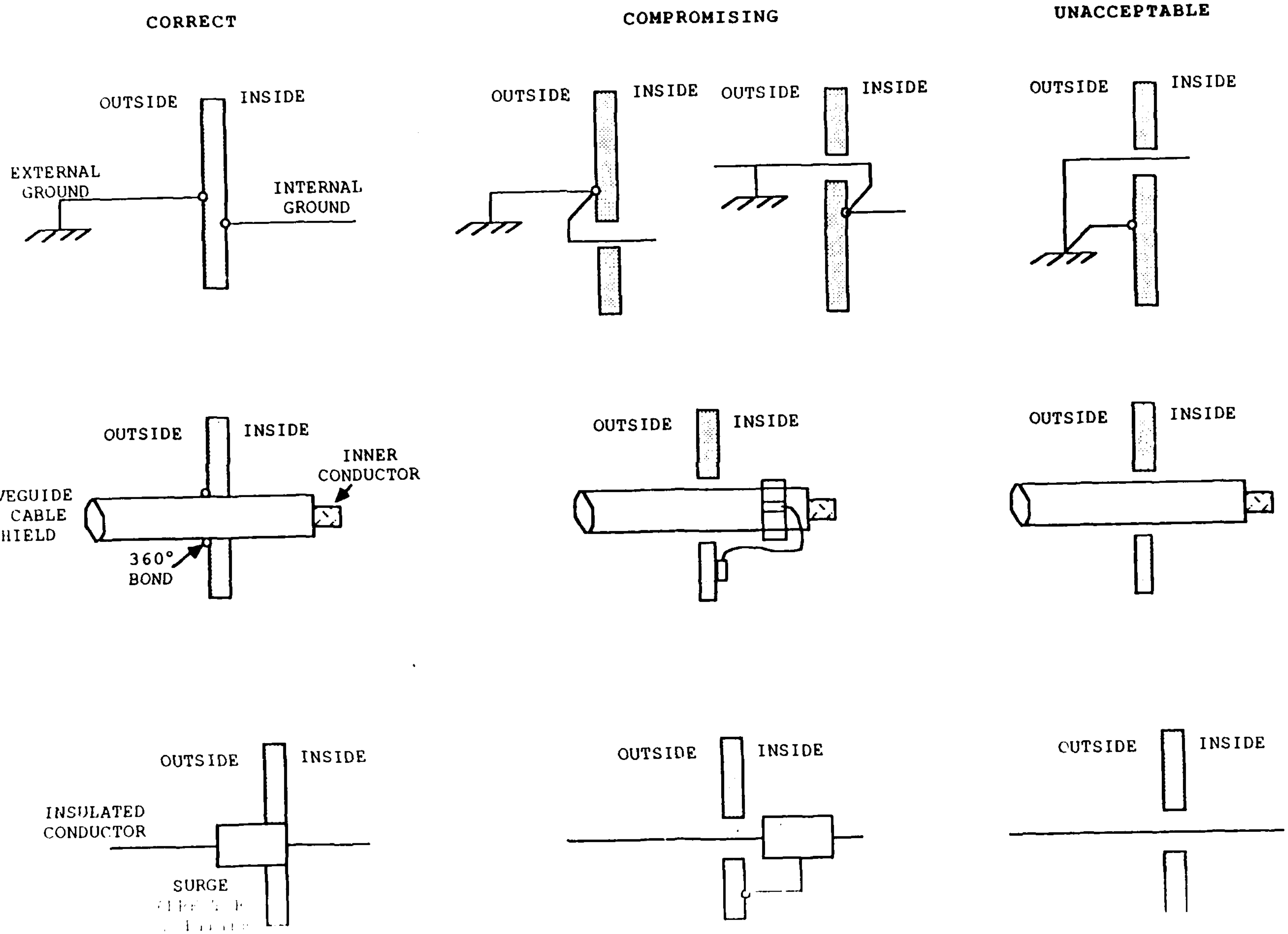


FIGURE 3.3-1. METHODS OF PENETRATING THE STRUCTURE WITH VARIOUS CONDUCTORS

Wiring is subject to differential mode and common mode coupling. Usage of twisted pair reduces the differential mode coupling. Shields tied to ground at each end of the cable significantly reduce the common mode coupling.

Figure 3.3-2 shows the coupling characteristics associated with various wire types and configurations. The wiring is assumed to be internal but routed near an aperture or non-metal structure.

Cable routing may not reduce transients from lightning indirect effects sufficiently to protect circuitry. Terminal protection devices to provide additional shielding can be placed at a vehicle penetration or within a circuit. Devices are typically in-line modules and may include limiters, filters, attenuators, buffers, and RF control devices. Each has different characteristics and must be evaluated for inclusion in specific designs. Important parameters, which should be evaluated for each device, are low shunt impedance, noise floor, insertion loss, insertion phase, and clamping capabilities at low and high levels.

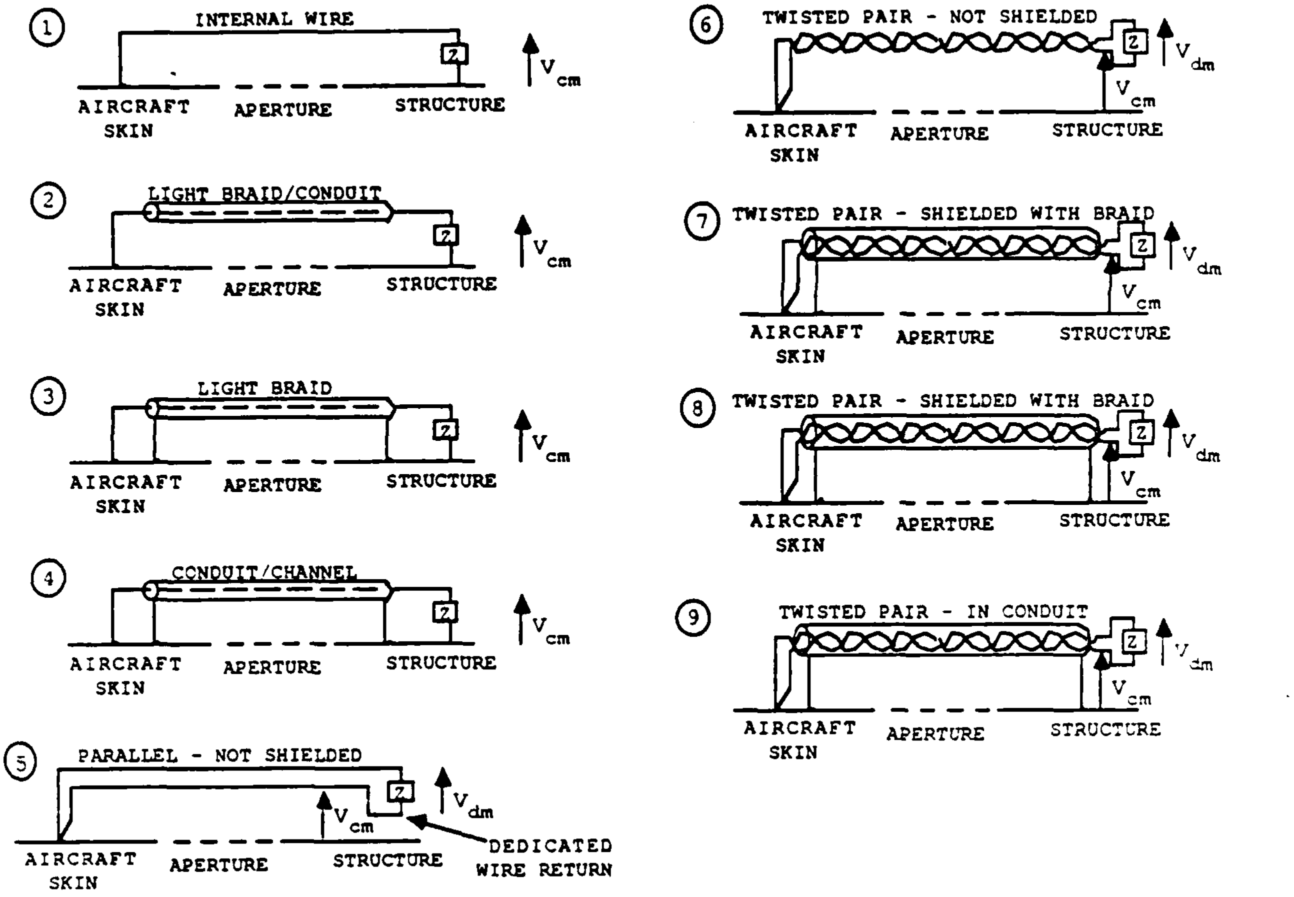
AEHP has defined the following guidelines for equipment installation to maximize the inherent shielding provided by the aircraft structure (Orange Book, 1987).

- Orient equipment where coupling with the EM fields is minimized. Avoid locations where fields are the highest (e.g., Zone 1 locations).
- Locate equipment as far from apertures and joints as possible.
- Cluster equipment in areas where the lowest flux density is expected, i.e., away from locations with small radii of curvature.
- Locate equipment in compartments with shielding, if possible.
- Where equipment must be located near apertures such as equipment bay hatches, the bay should be shielded and EMI gaskets used to improve bonding of the hatch to the compartment.
- Equipment in the canopy area, as well as the wiring leading to and from it, should be shielded. Equipment should be kept below the canopy sill, if possible.

A typical requirement for equipment protection is that both upset and damage protection be provided. This protection can be provided by either hardware or software.

The following AEHP guidelines apply to wire placement:

- Route the wiring in areas where lowest flux intensity is expected:
    - Within conductive structural enclosures.
    - Where minimum aperture coupling is predicted.
    - As close as possible to highly conductive structural members.



| | MAGNETIC FIELD INDUCTIVE/RESISTIVE VOLTAGES | ELECTRIC FIELD CAPACITIVE VOLTAGES |
|---|---|---|
| 1 | FULL COMMON MODE VOLTAGE | FULL COMMON MODE VOLTAGE |
| 2 | FULL COMMON MODE VOLTAGE | > 40 dB ATTENUATION |
| 3 | 20 TO 35 dB ATTENUATION | > 40 dB ATTENUATION |
| 4 | > 60 dB ATTENUATION | > 60 dB ATTENUATION |

| | COMMON MODE | DIFFERENTIAL MODE | COMMON MODE | DIFFERENTIAL MODE |
|---|---|---|---|---|
| 5 | FULL VOLTAGE | 20-30 dB LESS THAN Vcm | FULL VOLTAGE | NOT EASILY SPECIFIED, BUT 30-40 dB LESS THAN Vcm |
| 6 | FULL VOLTAGE | 50-55 dB LESS THAN Vcm | FULL VOLTAGE | |
| 7 | FULL VOLTAGE | 55-60 dB LESS THAN Vcm | > 40 dB ATTENUATION | NEGLIGIBLY SMALL |
| 8 | 20 TO 30 dB ATTENUATION | 55-60 dB LESS THAN Vcm | > 40 dB ATTENUATION | |
| 9 | > 60 dB ATTENUATION | > 60 dB LESS THAN Vcm | > 60 dB ATTENUATION | |

FIGURE 3.3-2. COMMON AND DIFFERENTIAL-MODE COUPLING CHARACTERISTICS FOR STRUCTURE RETURN AND TWO-WIRE CIRCUITS

  - Close to a skin that can be considered a good shield, such as aluminum with controlled joints.

  - Away from conducting structures with small radii of curvature.

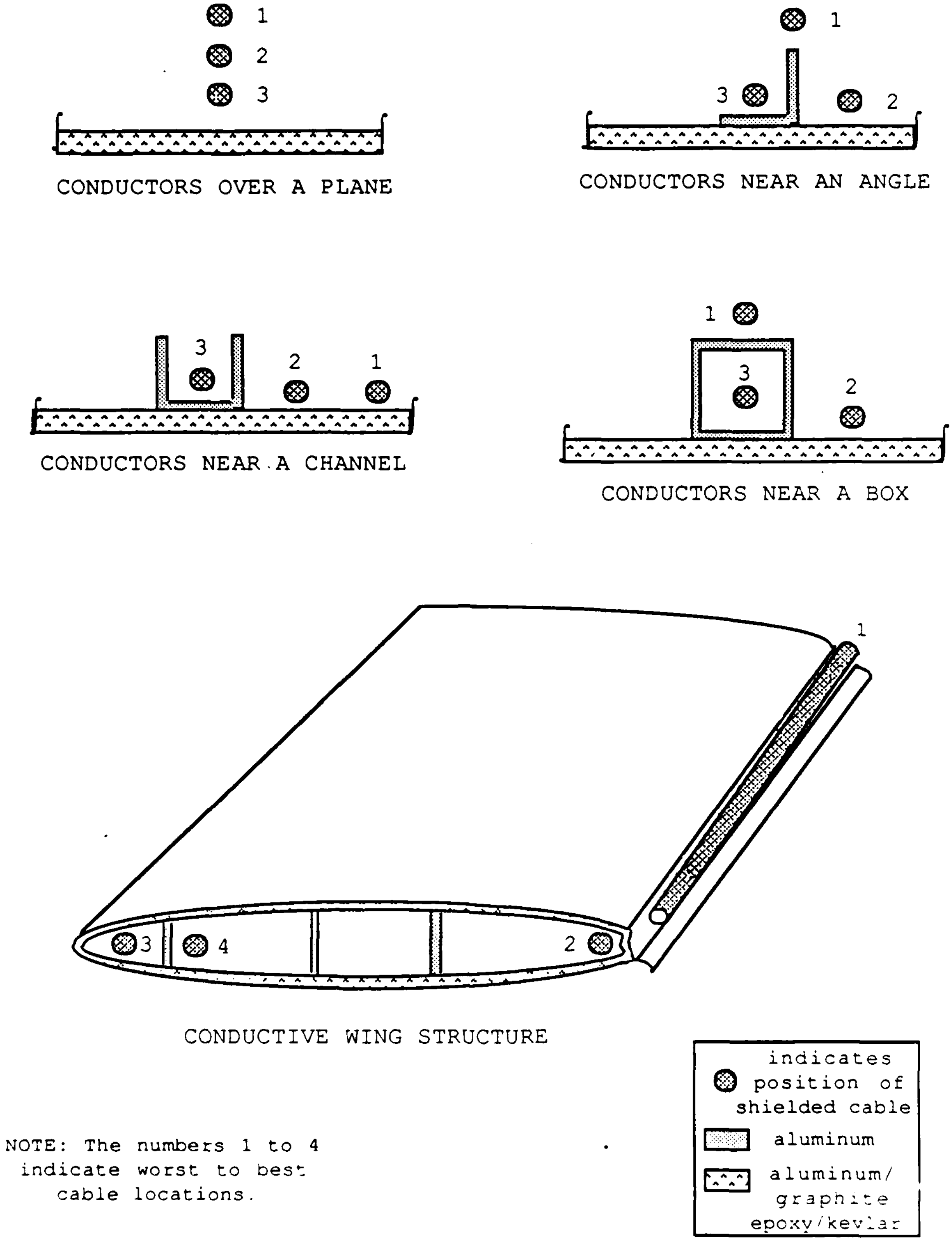
- Orient cables perpendicular to primary current path and joints to minimize coupling.

- Separate wiring according to degrees of hardness and threat exposure (i.e., isolate wiring to equipment located in a lightning zone).

Figure 3.3-3 shows various locations for routing cables near structure. For all-metal structures, the numbers 1 through 4 indicate worst to best locations for cables. This is not the case with composite structures.

Coupling to these config·:rations was quantified using a two-dimensional method-of-moments code (Geren, Melander, and Hall, 1987) using typical thicknesses and conductivities for aircraft structures. Predictions tabulated in table 3.3-1 were made based on three structural materials. First, each configuration was assumed to be entirely made up of aluminum. Second, the skin was assumed to be G/E and primary structure was aluminum. The third configuration was identical to the second, except that kevlar, a non-conductor, replaced the G/E skin. These predictions were made with only the structure shown and assumed a 200,000 amp double exponential waveform input to the model. The values illustrate the differences in cable placement for metal and composite structures. See section 6.1 for an additional example of coupling to wiring in various locations.

Peak current and voltage transient responses on wiring between aircraft systems, such as autopilot, engine control, fuel pump, fuel gauge, and electric power, due to a 200 kA direct lightning strike are tabulated in table 3.3-2. These values were obtained from results measured during a low-level swept CW lightning simulation test on a composite test bed representative of single engine general aviation aircraft (Cooley and Shortess, 1987). Wiring interconnections were representative of digital and analog signals, power, and grounds.


1
2
3
CONDUCTORS OVER A PLANE
1
3
2
CONDUCTORS NEAR AN ANGLE
3
2
1
CONDUCTORS NEAR A CHANNEL
1
3
2
CONDUCTORS NEAR A BOX
1
3
4
2
CONDUCTIVE WING STRUCTURE
● indicates position of shielded cable
▨ aluminum
▨ aluminum/graphite epoxy/kevlar

NOTE: The numbers 1 to 4 indicate worst to best cable locations.

FIGURE 3.3-3. CABLE ROUTING NEAR CONDUCTIVE STRUCTURE

TABLE 3.3-1. ESTIMATED SHIELD CURRENTS DUE TO A DIRECT LIGHTNING STRIKE

| Aluminum Skin | | | Graphite Epoxy Skin | | | Kevlar Skin | | |
|---|---|---|---|---|---|---|---|---|
| Shield Location | Peak Current (kA) | Peak Time (μs) | Shield Location | Peak Current (kA) | Peak Time (μs) | Shield Location | Peak Current (kA) | Peak Time (μs) |
| Shields over a plane | | | | | | | | |
| 1 | 4.76 | 6 | 1 | 110 | 50 | 1 | 200 | 6 |
| 2 | 3.67 | 6 | 2 | 110 | 50 | 2 | 200 | 6 |
| 3 | 2.48 | 6 | 3 | 110 | 50 | 3 | 200 | 6 |
| Shields near an angle | | | | | | | | |
| 1 | 5.91 | 6 | 1 | 33.8 | 30 | 1 | 50.3 | 6 |
| 2 | 2.51 | 6 | 2 | 39.4 | 30 | 2 | 57 | 6 |
| 3 | 2.46 | 6 | 3 | 13.6 | 32 | 3 | 21.7 | 6 |
| Shields near a channel | | | | | | | | |
| 1 | 3.05 | 6 | 1 | 46.7 | 20 | 1 | 55.4 | 6 |
| 2 | 1.00 | 6 | 2 | 20.6 | 30 | 2 | 30.5 | 6 |
| 3 | .77 | 6 | 3 | 4.62 | 32 | 3 | 6.7 | 6 |
| Shields near a box | | | | | | | | |
| 1 | 4.32 | 6 | 1 | 17.9 | 26 | 1 | 26.2 | 6 |
| 2 | 2.14 | 6 | 2 | 35.6 | 24 | 2 | 46.4 | 6 |
| 3 | .04 | 104 | 3 | .88 | 124 | 3 | .88 | 108 |
| Shields in a wing | | | | | | | | |
| 1 | 10.5 | 6 | 1 | 35.9 | 30 | | | |
| 2 | .38 | 16 | 2 | 35.9 | 32 | | Not Calculated | |
| 3 | .02 | 112 | 3 | 3.4 | 28 | | | |
| 4 | .46 | 12 | 5 | 28.4 | 20 | | | |

TABLE 3.3-2. COUPLING RESPONSES TO SUBSYSTEM WIRING DUE TO A DIRECT LIGHTNING STRIKE

| System | Coaxial (RG-58) | Twisted Pair (no shield) | Twisted Pair (shielded) | Twisted Triple (no shield) | Single Wire |
|---|---|---|---|---|---|
| Nose-to-Tail Attachment | | | | | |
| Fuel Electrical | 100-300 V<br>35 A | | | | |
| Fuel Mechanical | | | 30-210 V<br>10 A | | |
| Engine Control | 10-50 V<br>800 A | | 55 V | | |
| Lights Power | | | | 40-1500 V<br>15-50 A | |
| Autopilot | | 50-1070 V | 50-230 V<br>1800-7000 A | | 540 V |
| Autopilot shield disconnected | | 550-2400 V | 250-1600 V | | 1300 V |
| Wing-to-Tail Attachment | | | | | |
| Fuel Electrical | 800-2600 V<br>20 A | | | | |
| Fuel Mechanical | | | 90-1200 V<br>60 A | | |
| Engine Control | < 10 V<br>140 A | | 150-400 V | | |
| Lights Power | | | | 10-32,000 V<br>15-210 A | |
| Autopilot | | 1100-1070 V | 250-2600 V<br>15,000-60,000 A | | 1850 V |
| Autopilot shield disconnected | | 1500-20,000 V | 700-11,000 V | | 2500 V |

# 4. INDIRECT EFFECTS PROTECTION - TEST METHODS

## 4.1. Review of Lightning Simulation Methods

This section presents a review of the lightning simulation technology used for evaluating the effects of lightning and static electrification on aircraft. The evolution of the simulation technology and considerations in selecting a simulation technique are discussed.

### 4.1.1. Lightning Simulation Technology

Several lightning simulation test techniques are currently being utilized for verification and validation of aircraft lightning protection. These different methods are the outgrowth of research using ground based simulations of lightning interactions with aircraft in flight. Under these test methods several aspects of natural lightning are simulated by pulse generators having various waveshapes and energy content as well as swept CW generators. The methods are often utilized, singly and in combinations, throughout an aircraft development cycle. These test methods, together with analysis procedures, characterize the indirect effects of lightning on aircraft electrical/electronic equipment.

The main reason for the different test methods is the difficulty of accurately generating natural lightning in the laboratory for large sized objects. It is very difficult (if not impossible) to accurately simulate severe lightning environments on an aircraft. This is because of the high levels of energy, current, and electric and magnetic fields associated with naturally occurring lightning. Simulation of these high energy levels requires very large and expensive facilities for an object the size of an airplane. Tests on aircraft and electrical/electronic equipment more commonly attempt to simulate portions of the lightning environment.

High level simulations of lightning appropriate for protection against direct effects, such as structural damage, are easier to implement because only small portions of the aircraft need to be exposed during a test. These simulations for direct effects of lightning on aircraft have been codified and are generally accepted as published in the report of the SAE Committee AE4L (1978).

Simulations for indirect effects, such as for the potential damage to flight control electronics from induced electrical transients, could require the use of the entire aircraft and several attachment locations for full evaluation. Thus, simulations for the indirect effects of lightning on aircraft and hardware have evolved along with the research efforts leading to a better understanding of these effects. It was recognized early on that electronic equipment would be affected by induced transients from lightning and other EM energy. However, the aircraft developments were allowed to go forward while answers were sought for protection against these effects. Research efforts were initiated in the mid 1970's to develop the means of testing, assessing, and protecting the advanced electronics equipment. Since indirect effects testing necessarily involves the full vehicle and simulation of severe lightning levels on the full vehicle is impractical, approximate test methods were sought.

Several different investigators arrived at a variety of simulation techniques and test equipment because of different starting points and available resources. The data in table 4.1-1 summarizes the prior research and development tests on full scale aircraft. Major research and development efforts were concentrated in the AEHP program sponsored by the Air Force Flight Dynamics Laboratory (AFFDL) and supported by Tri-Services, FAA, NASA, and the Defense Nuclear Agency (DNA).

### 4.1.2. Considerations in Selecting Simulation Techniques

Many techniques and facilities are currently available for simulation of atmospheric electricity effects on aircraft. The selection of an appropriate method is challenging; it depends upon the ultimate use of the data and state of development of an aircraft.

Existing techniques for simulating static electrification, such as precipitation static, provide adequate data for aircraft design and protection. Nearby lightning strikes may be simulated using simulators developed for Electromagnetic Pulse (EMP) tests. The real challenge is to adequately simulate effects of lightning directly attached to an aircraft. A simulation technique that imposes all features of the lightning environment in a proper time sequence is desirable for full aircraft level tests. However, full vehicle tests are not time- and cost-effective for subsystem tests or to provide design data. It is especially important that the simulation technique provide data on the system, subsystem, component equipment, or Line Replaceable Unit (LRU). This data can be extrapolated to the values that occur when the aircraft is exposed to the real lightning environment.

Lightning simulation techniques must account for the significant features of natural lightning and the natural EM environments. These environments ultimately determine the indirect effects on advanced aircraft electronic equipment. Features necessary in the simulation setup include:

- The number of strokes in a lightning flash and the time between them.
- The peak current amplitude, rise time, and decay time reflecting parameters recently measured on natural lightning strikes.
- The proper EM environment geometric configuration around the test bed and the proper time phasing.
- The high voltage and electric fields associated with approaching leaders and static charging, preceding the high current and magnetic fields associated with the lightning return strokes.
- Lightning channel impedance and attachment.

TABLE 4.1-1. PRIOR RESEARCH AND DEVELOPMENT TESTS ON FULL-SCALE AIR VEHICLES

| TEST | DESCRIPTION | RESULTS |
|---|---|---|
| AFFDL F-16<br>Mockup; G/E<br>Composite<br>1983 | Direct Attached<br>- Coaxial<br>- CW Tests<br>- Moderate Threat 20 kA; 50 kA/μs | - V, I, B-Dot, D-Dot Data<br>- Detailed Model<br>- CW response within 4 dB of measurements at 28 kA |
| AFFDL ALCM<br>1983 | Direct Attached<br>- Coaxial<br>- Full Threat 200 kA; 200 kA/μs<br>- Moderate-Level 50 kA | - V, I Data<br>- EM Model<br>- Extrapolated values 7.7 dB greater than measurements at 200 kA |
| NASC F/A-18<br>1982 | Direct Attached<br>- Coaxial<br>- High-Level 100 kA; 100 kA/μs<br>- Low-level CW 760 A | - Functions<br>- V, I Data<br>- EM Model<br>- No Upset/Damage<br>- Predicted CW results 7.2 dB greater than measurements at 173 kA |
| NASC F-14<br>1982 | Direct Attached<br>- Coaxial<br>- High-Level 180 kA; 180 kA/μs | - Functions<br>- V, I Data<br>- EM Model<br>- Predictions |
| NASA F-106<br>Calibration<br>1982 | Direct Attached<br>- Shock-Excited<br>- Radiated | - V, I, B-dot, D-dot Data<br>- Spectral Analysis<br>- Simple Model |
| RAE UK JAGUAR<br>1982 | Direct Attached<br>- Damped Sine Wave<br>- Several Levels 100 kA; 20 kA/μs | - V, I, E, H Data<br>- Spectral Analysis<br>- External Currents/Fields |
| NSWC F-16<br>Mini-Test<br>1982 | Direct Attached<br>- Low-level 30 kA; 30 kA/μs | - Currents<br>- Spectral Analysis |

TABLE 4.1-1. PRIOR RESEARCH AND DEVELOPMENT TESTS ON FULL-SCALE AIR VEHICLES (continued)

| TEST | DESCRIPTION | RESULTS |
|---|---|---|
| AFFDL C-130<br>1981 | Direct Attached<br>- Radiated<br>- Low-level | - B-dot, D-dot Data<br>- Simple Models |
| AFFDL F-111<br>1978 | Direct Attached<br>- Low-level; 2.5 kA | - Voltages<br>- Simple Model |
| AFFDL YG-16<br>Composite; Fwd. Fuselage; 1978 | Direct Attached<br>- Moderate to High-Level 30-100 kA; 100 kA/μs | - Voltages and Fields<br>- External EM Models |
| AFFDL A-7<br>1977 | Direct Attached<br>- Low-level 2 kA; 1.25 kA/μs | - Voltages<br>- Simple Model |
| GENERAL DYNAMICS F-16<br>1975 & 1976 | YF-16 #1,2 Lightning Tests<br>2-30 kA; 50 kA/μs | - Voltages<br>- Simple Model |
| NASA F-8<br>1975 | Direct Attached<br>5 kA; 5 kA/μs | - Voltages<br>- Data Analysis |
| UH-60<br>Helicopter | Direct Attached<br>- Low-level; 5 kA | - Unknown |
| 757 Transport | Direct Attached<br>- Low-level CW Test 250 A | - Spectral Analysis |
| ACAP<br>Helicopter | Direct Attached<br>- Low-level CW Test < 20 A<br>- Moderate-level Pulse 24 kA; 18 kA/μs<br>- High-level Pulse 200 kA; 146 kA/μs | - Spectral Analysis<br>- Voltages, Currents, and Fields<br>- EM Models<br>- Extrapolated CW results 6 dB greater than measurements at 200 kA |

- Voltage and current levels high enough to excite arcs and nonlinear effects, if any.

It is not possible to meet all these requirements with any one of the simulation techniques cu:rently in use. The best present techniques only satisfy a few of the above requirements in any one setup.

The desired output from the lightning simulation technique determines which of these features are implemented and the degree of analysis required to demonstrate lightning protection. For example:

- Full vehicle, severe lightning protection demonstration tests with a minimum of analysis require simulation of the extreme values for the lightning parameters.

- Protection design demonstration tests can be performed with lower levels of pulse or with frequency domain measurements but require the support of analysis.

- Avionics and equipment susceptibility can be determined using bench tests on equipment outside the aircraft under test but require analysis or additional testing to relate to specific vulnerabilities of any aircraft.

The most widely applicable simulation methods are the pulse testing at various levels and rates of rise and the swept CW testing. The CW method differs from the pulse methods in the type of generator used and in the amount of analysis needed for interpretation of the data.

## 4.2. Lightning Pulse Generator Techniques

Many pulse techniques exist for generating simulations of lightning waveforms to investigate the induced effects of lightning on aircraft and avionic equipment. These techniques are based on discharging a high voltage source into the test aircraft, using switches and wave shaping elements to produce the appropriate current waveform. Most lightning simulators use variations of an RLC circuit to produce some of the relevant lightning characteristics. The circuit may be configured in either the underdamped, critically damped, or overdamped configuration. Four variants of the RLC circuit are in use today: the linear damped sine wave, the critically damped, the double exponential, and a nonlinear generator having sine wave rise and an exponential tail.

The underdamped RLC circuit generates the fast rise times and a moderate-level action integral desired with a practical circuit, but the waveform is oscillatory rather than unipolar as in natural lightning. J. Robb of Lightning and Transients Research Institute (LTRI) and B. Burrows of Culham Laboratory (England) have used damped sine wave pulsers for achieving high currents and fast rise-times (Riley et al., 1984).

The critically damped circuit gives a unipolar waveform, but the decay-time to rise-time ratio is smaller than that of natural lightning. However, the simplicity of constructing this type of pulser makes it attractive to generate a moderate-level pulse. With a low inductance aircraft and return circuit this type of pulser can provide moderate rise-times and peak currents. The AFFDL has built moderate-level pulse generators using the standard RLC circuit arrangement. Significant improvements to the pulse generator switch and transient measurement system have been incorporated into this system (Walko, 1974).

An overdamped circuit requires a large amount of stored energy to produce the desired waveform. Therefore, this configuration is generally not used to provide both fast rise times and high current levels on a single pulse. B. Burrows utilized a pulse generator with an overdamped RLC circuit. This arrangement was combined with an approximately coaxial return conductor arrangement to produce moderate-level current pulses of 20 kA with a peak rate-of-rise 170 kA/μs (Butters, et al., 1982). Field distribution calculations were used to determine the placement for the return conductors.

The nonlinear "crow-bar" generator provides an efficient means for generating high peak currents with high energy in the decay. The sine wave efficiently transfers energy from the main capacitor bank into the test aircraft inductance. This energy is then short circuited by a spark gap and discharges with a Resistive/Inductive (RL) decay, producing the long decay tail on the test airplane's current pulse. Sandia National Laboratories has built a high-level lightning simulator for the Department of Energy (DOE) using a crowbar circuit design. This produces an essentially nonlinear circuit, because before the crowbar switch is closed it is an RLC circuit and after the switch is closed, an RL circuit.

An evaluation of four simulation methods for testing for indirect effects of lightning on full-size aircraft, having advanced technology structural materials and electronics equipment, is given in Cooley and Shortess (1987). The capabilities and limitations of these methods are summarized in table 4.2-1. A detailed description of each test method is given in the following sections.

### 4.2.1. Low-Level Swept Continuous Wave

This lightning simulation technique utilizes a CW rather than a pulse to excite the transients. Because the levels of testing are generally at low levels of current relative to the severe threat lightning current, there is more uncertainty. Consequently, more analysis is required to extrapolate to severe current levels.

Basically, this method utilizes a network analyzer to measure transfer functions (amplitude and phase) from a lightning attachment point to test points (voltage or current) within the aircraft. Figure 4.2-1 shows an example test setup.

The transfer functions, measured over a wide frequency range, are subsequently processed by multiplying by the severe lightning current spectrum to develop test point spectral responses. The test point responses are then numerically Fourier transformed to generate the pulse response expected from severe lightning. The method is generally applicable to other EM threats as well. Standard swept CW network analyzers provide coupling transfer function data as amplitude and phase versus frequency.

TABLE 4.2-1. SUMMARY OF SIMULATION TECHNIQUE CAPABILITIES

| | LOW LEVEL | | | HIGH LEVEL |
|---|---|---|---|---|
| REQUIRED FEATURES FOR DIRECT STRIKE SIMULATION ON FULL VEHICLES | SWEPT CW BENCH TEST | FAST-RISE PULSE TEST | SHOCK EXCITATION | FAST-RISE PULSE TEST |
| 1. High Voltage - E Field Phase Simulating a Leader Stroke | Linear Only | Limited By Pulse | Limited By Pulse | OK |
| 2. High Current - H Field Simulating a Return Stroke Represented by Component A | Yes | Yes | Yes | OK |
| 3. Continuing Currents Which Link Successive Return Strokes Represented by Component C | Yes | Yes | Yes | OK |
| 4. Fast Rise Times (30 - 100 ns) To Match Recent Measurements | Yes | Yes | Yes | Limited By Pulse |
| 5. Coaxial Transmission Line Test Setup of Test Object/Return Circuit | | | | |
| • Simulation of In-Flight Conditions | Yes | Yes | ? | Yes |
| • Simulation of Uniform Currents and Fields | Yes | Yes | ? | Yes |
| 6. Lightning Channel Attachment | Yes | Limited By Pulse | Limited By Pulse | Limited By Pulse |
| 7. Test for Equipment Functional Responses | | | | |
| • Upset | Yes | No | ? | Yes |
| • Damage | Yes | No | ? | Yes |
| 8. Adapt Data to New Threat Parameters | | | | |
| • EM Coupling | Yes | Limited By Pulse | Limited By Pulse | Limited By Pulse |
| • Functional Responses | Yes | Limited to Observed | Limited to Observed | Limited to Observed |

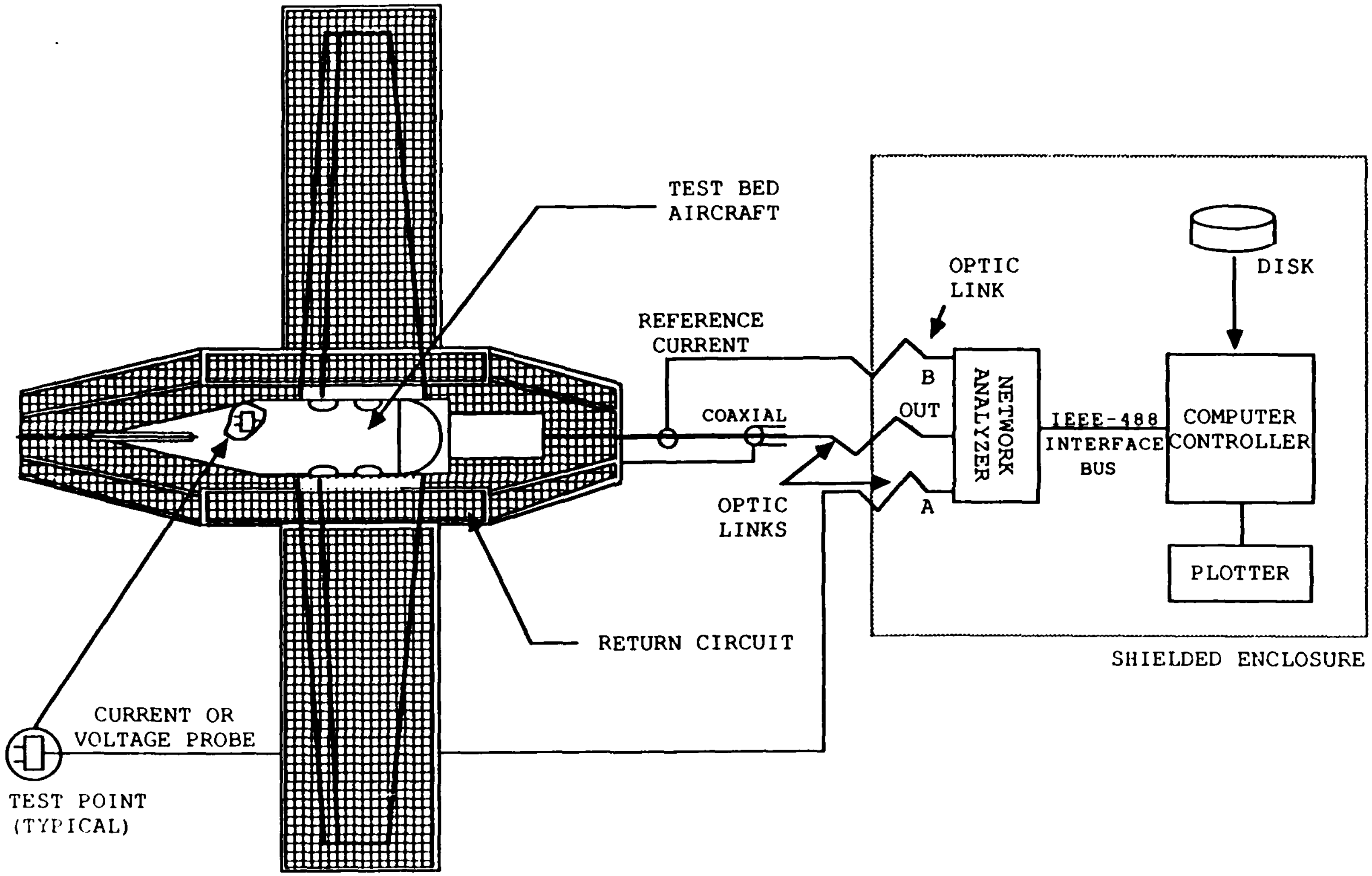


FIGURE 4.2-1. TYPICAL LOW-LEVEL SWEPT CONTINUOUS WAVE TEST SETUP

Figure 4.2-2 provides an example of measured transfer function data, (a), and the pulse response, (d), obtained by Fourier transform processing of the CW measurement. This analysis requires a significant amount of numerical processing to extrapolate values to in-flight results. The intermediate data processing steps are illustrated in (b) and (c). Between 10 and 100 MHz in (a), the noise becomes more dominant than the signal. Here a judgement must be made as to the validity of the data. If the data are not valid, an estimate of the signal response must be made over the frequency range in question. The plot in (b) shows the expected signal with the noise removed. The 200 kA double exponential threat convolved with data in (b) is shown in (c). Fourier analysis of this spectrum yields the pulse response in (d).

A principal advantage of the CW test method is the low level of injected current that can be applied (a few amperes) while attaining a high level of signal-to-noise ratios. Low levels of current can be used because of the wide frequency range contained in the lightning induced transient's interaction and coupling within the aircraft. Therefore, the energy delivered to the test object can be averaged over a relatively long time compared to pulse methods. This averaging provides an improved signal-to-noise ratio particularly when a narrow band receiver is used in the network analyzer.

Due to the transfer function complexity for most coupling responses, data are much easier to understand when obtained with CW measurements versus pulse techniques. The transfer function complexity contains clearly displayed and quantified resonances, superior signal-to-noise ratios, and lower required generator levels than the pulse methods. Under the CW method, an attached current of a few amperes can provide as high a signal-to-noise ratio as a severe lightning pulse. With these low levels of testing the CW measurement method offers several advantages for obtaining parametric sensitivity data, for example, the quick evaluation of a variety of mock-up protection options.

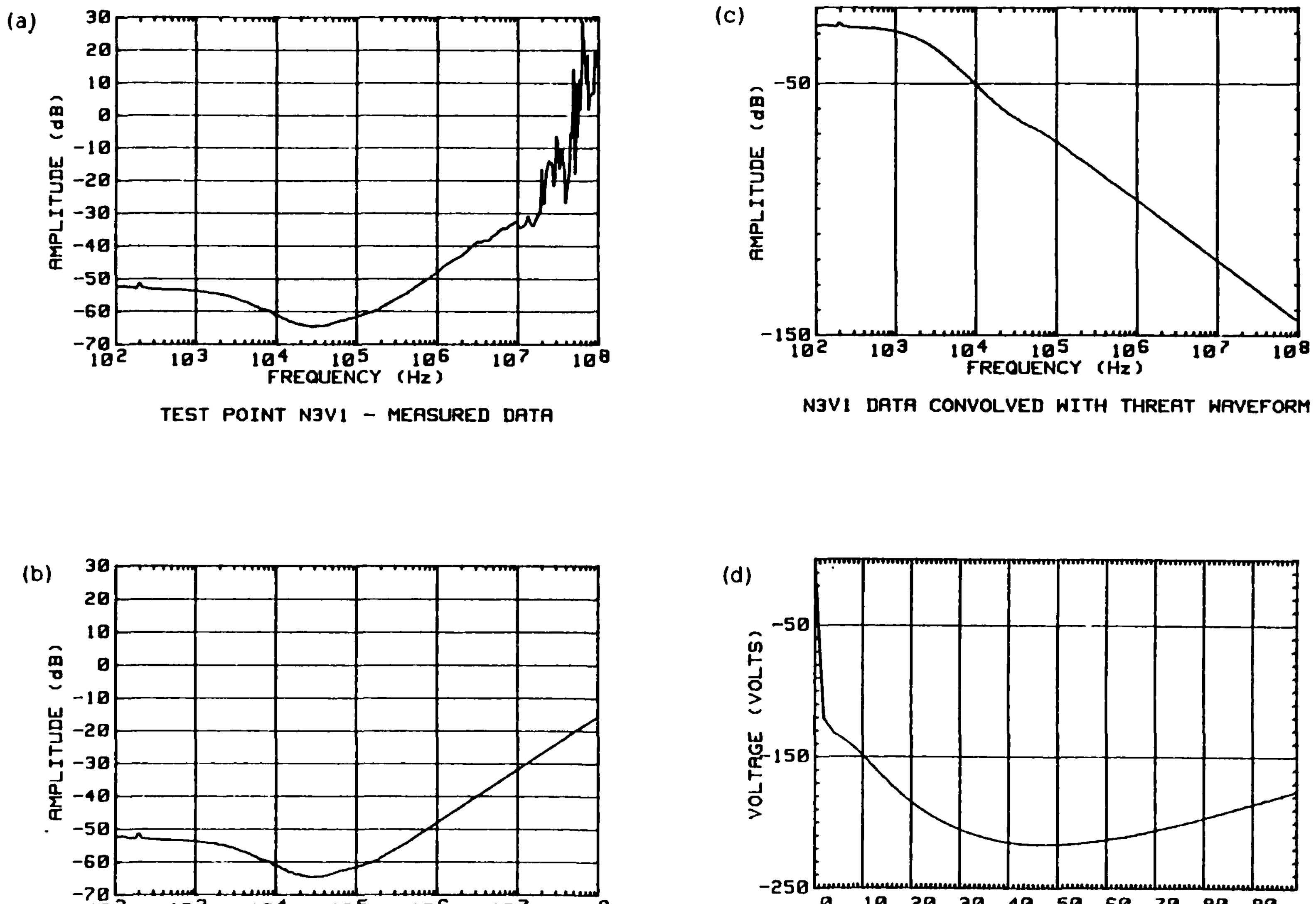
Nonlinearities, such as arcing and sparking at joints, are not represented with this test method because of the low currents injected. However, it has been demonstrated that extrapolated results from CW measurements are six to eight dB more conservative than higher level pulse measurements (Shortess, Cooley, and Melander, 1988 and Walen, 1988).

Swept CW measurement techniques for full vehicle lightning protection design demonstration are as follows:

- Conduct time-delay-reflectometer (very low-level pulse) measurements to identify apertures and locations where EM coupling occurs.

- Conduct CW measurements to measure transfer functions from the external lightning current attachments to the EM coupling sources, and develop transfer functions from the sources to wiring and from the wiring to equipment.

- Combine the CW measured transfer functions with a model of the external lightning threat to obtain an overall computer model for EM response prediction.



TEST POINT N3V1 - MEASURED DATA

N3V1 DATA CONVOLVED WITH THREAT WAVEFORM

TEST POINT N3V1 - SMOOTHED DATA

FOURIER TRANSFORMED PULSE RESPONSE

FIGURE 4.2-2. EXAMPLE TRANSFER FUNCTION ANALYSIS SEQUENCE

- Excite the computer models with the applicable severe lightning current spectrum and transform to time domain determining the full-threat level transients at critical circuits.

- Perform bench tests (induced cable current or pin voltage injection tests), using the predicted severe lightning pulses (possibly including timing from apertures and restrikes), at critical circuits on the aircraft.

- Determine protection design margins for the equipment. If the protection is inadequate, determine designs to reduce transients or reduce equipment susceptibility to the transients.

This method is also applicable to evaluating coupling coefficients for the high-voltage leader-attachment phase and nearby strike, as well as for the high-current phase by means of piece-wise linear simulation techniques. For these techniques, the generator, airplane, and return circuit are configured to represent the EM environment for each of the phases, one at a time. The coupling parameters included for the current and EM fields response of a given subsystem to the various aspects of the threat may be used to define the appropriate threat waveforms for a bench test. These time-ordered threats may then be imposed upon the component or subsystem in the proper sequence.

### 4.2.2. Low-Level Fast-Rise Pulse

Under this method, current pulses are generated by means of a pulse generator that is tightly coupled to the test aircraft (see figure 4.2-3). For this application, the test aircraft return circuit inductance and pulse generator capacitance combine to provide a critically damped circuit. This results in a current pulse having a high rate of rise with a relatively short decay time. The parameters are chosen so that the peak rate-of-rise matches the rate-of-rise for severe lightning currents while the peak amplitude matches the peak amplitude for low levels of lightning current. The generator decay time is much faster than natural lightning.

This simulation provides stress levels that match the severe rate-of-rise of natural lightning. This is appropriate when the principal EM coupling mechanism is mutual inductance or mutual capacitance, as is the case for balanced circuits isolated from structure. For composite structures where the coupling mechanism may be due to resistive drops, the simulated currents are not high enough to match the expected levels of moderate lightning strikes.

Since such a generator produces less than a moderate lightning stress on much of the equipment in an aircraft, the survival of equipment under the test condition only provides confidence in the capability to survive minor lightning strikes. The low-level of current injected will not be sufficient to cause non-linear responses, functional upset, or damage responses.

Careful analysis and interpretation of the test data is necessary to provide confidence in the capability to survive severe lightning strikes. This analysis must include interpretations of the coupling mechanism (I-dot or I) for each cable run and equipment area on the aircraft. The coupling mechanisms are necessary to extrapolate measured voltages and currents to higher severe

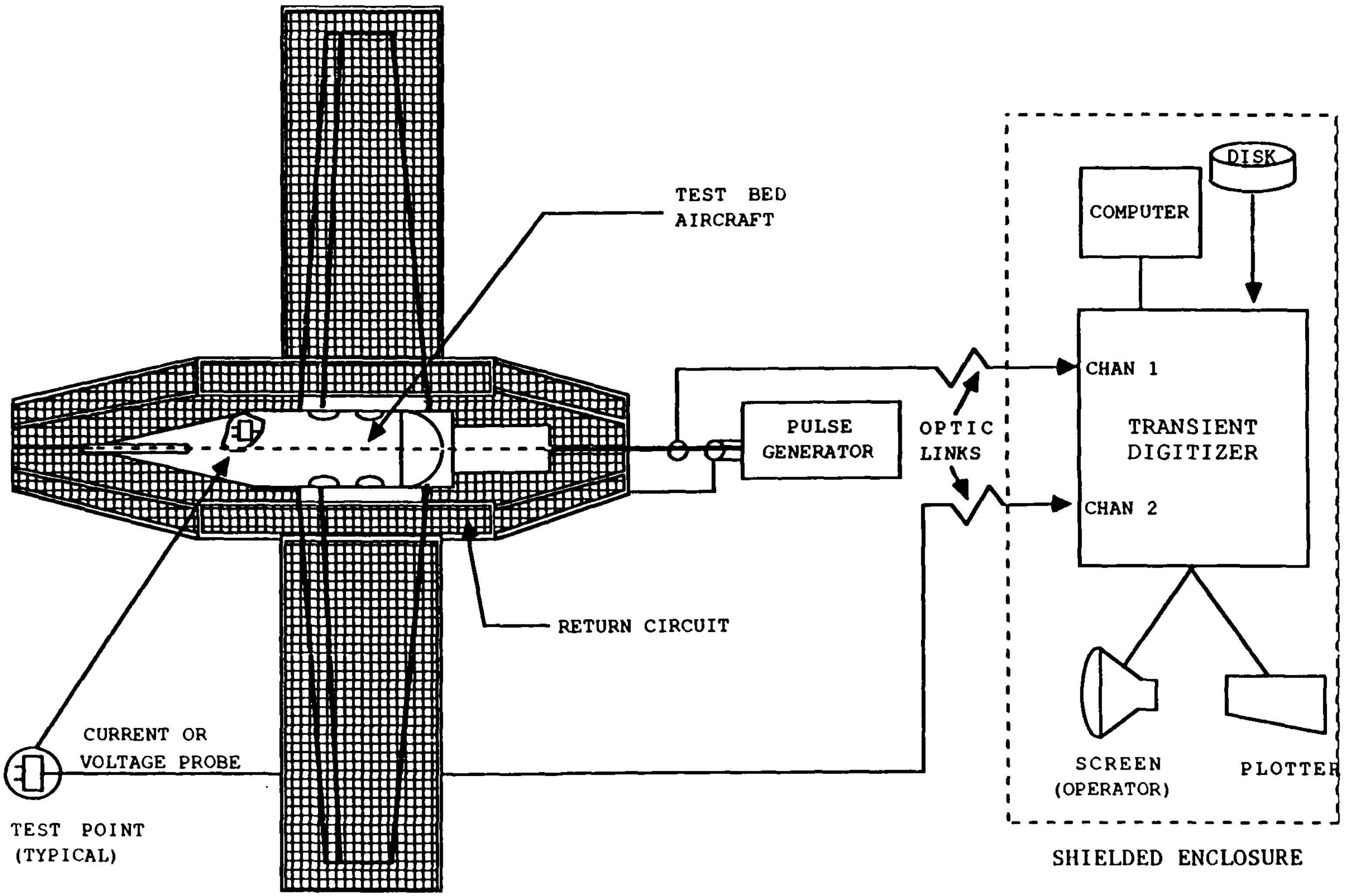


FIGURE 4.2-3. TYPICAL PULSE SIMULATION TEST SETUP

lightning responses. The I-dot driven responses scale according to the rate-of-rise parameters while the resistive driven responses scale according to I parameters. For many responses it will be found that they are driven by both I and I-dot coupling mechanisms. Since the generator circuit is tightly coupled to the aircraft under test, it may not be possible to separate the I and I-dot coupling from the data. This is because the internal coupling in the aircraft provides a different scale factor for I and I-dot at different test points, due to internal RLCM parameters, as opposed to the fixed I/I-dot parameters built into the generator. Therefore, the separation of the test results into purely I or I-dot will not be possible without considerable test efforts using different generator parameters.

If the generator waveform parameters match lightning parameters except for peak amplitude, then the response can be scaled by a multiplicative constant. For any other generator or choice of waveform parameters this will not be the case.

Based upon linearity arguments, Walko (1974) developed such a test based upon the use of a very low-level double exponential current pulse with a peak magnitude as low as 200 A. If rise and fall time constants match the values for lightning, then this current pulse theoretically contains all of the frequency components of a 200,000 A waveform in proper proportion, thereby allowing transients to be scaled linearly. The pulse is passed through the aircraft structure (from nose to tail, for example). The resulting transients produced on critical wire runs inside the aircraft are monitored by connecting voltage/current measurement instrumentation across the circuit to be monitored. The peak values of the measured transients are then extrapolated upward to the severe lightning current level. In the case of a 200 A, 6 x 70 microsecond test pulse, the peak levels are multiplied by 1000 to determine the anticipated transients for a 200,000 A strike with the same waveform. Since the test wave shape is the same as the threat waveform, the I-dot and the peak current, I, have the same scaling factor. This is illustrated for 200 kA and 200 A double exponential current pulses in figure 4.2-4.

Unless the generator rise and fall time constants match lightning parameters, it is probably better to use the basic measured responses as representative of a low to moderate lightning stress and not try to extrapolate the measured responses to higher levels.

The most accurate approach to extrapolation of the voltage and current measurements to higher levels of stress is through an analytical model based upon electrical equivalent circuits. This approach to modeling is similar to the analysis required for the CW method. The major difference is that the measured data for comparison with the models is derived from the pulse measurements.

The digital recording equipment used to acquire data from pulse testing typically has a dynamic range of only 40 dB. This is several orders of magnitude less than the dynamic range obtainable when measuring in the frequency domain.

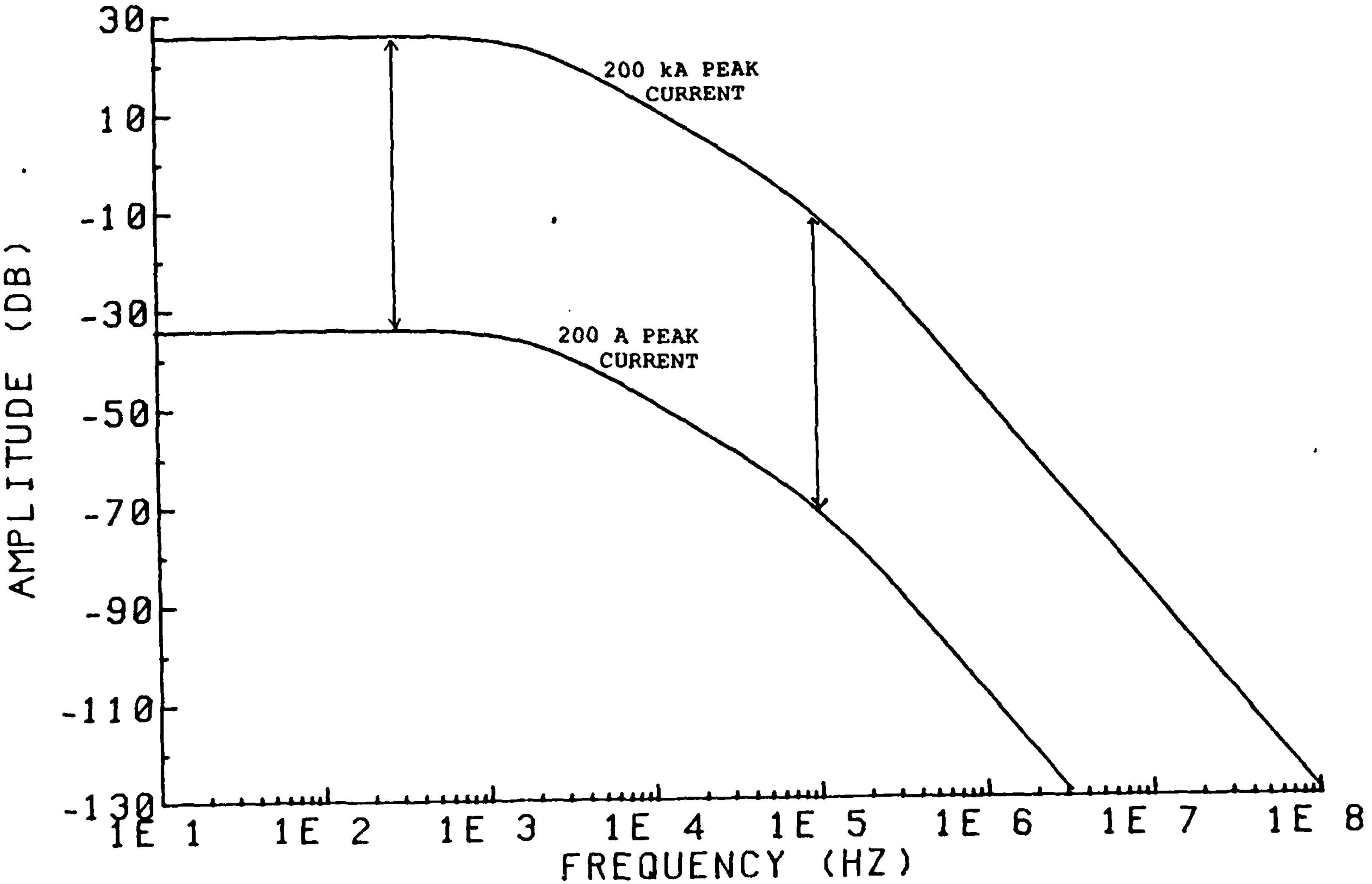


FIGURE 4.2-4. COMPARISON OF FREQUENCY SPECTRA

Low-level pulse measurement techniques for full vehicle lightning protection design demonstration are as follows:

- Conduct time-delay-reflectometer (very low-level pulse) measurements to identify apertures and locations where EM coupling occurs.

- Conduct CW measurements to measure transfer functions from the external lightning current attachments to the EM coupling sources. Develop transfer functions from the sources to wiring and from the wiring to equipment.

- Combine the CW measured transfer functions with a model of the low-level pulse generator to obtain an overall computer model for EM response prediction of the test responses.

- Compare the measured pulses with the model predictions to provide confidence in the computer models. Determine the error bars in the model responses from the measurement comparisons.

- Excite the computer models with the applicable severe lightning current spectrum and transform to time domain determining the full-threat level transients at critical circuits.

- Perform bench tests (induced cable current or pin voltage injection tests), using the predicted severe lightning pulses (possibly including timing from apertures and restrikes), at critical circuits on the aircraft.

- Determine protection design margins for the equipment. If the protection is inadequate, determine designs to reduce transients or reduce equipment susceptibility to the transients.

It should be noted that second and third bullet items utilize results from CW testing. Bullet items utilizing the CW method provides a higher degree of confidence in the modeling of the various coupling mechanisms. The pulse data could also be used to refine the models but there would be lower confidence in the extrapolation using a model that had been refined with the pulse test alone. This is due to the difficulty of separating the various RLCM parameters from the time domain test responses.

### 4.2.3. High-Level Fast-Rise Pulse

Under this method, current pulses are generated by means of a large pulse generator that is tightly coupled to the test aircraft and return circuit. There is considerably more energy required in the main pulse generator for this method than the low-level fast-rise test method. In the usual application, the test aircraft and return circuit resonate with the pulse generator capacitance to provide high rate-of-rise current pulses having a damped sinusoidal waveform. The generator and return circuit parameters are chosen so that the pulse rise time matches the rise time for severe lightning currents. The peak amplitude is near enough to the severe lightning current levels that the data extrapolations can be made with high confidence. The generator decay time can be adjusted to the same as natural lightning or much faster than natural lightning.

This simulation provides levels at and above the moderate lightning strike current amplitude. This test method is appropriate when the amount of analysis is to be minimized. The analysis provides high confidence in the survival of the aircraft and equipment under severe lightning strikes.

The high-level pulse simulation technique provides a level of stress that is somewhat greater than the expected value for lightning strikes. This test stress increases the confidence in the protection design over that of a low level test technique used alone. For example, portions of the protection system, such as cable shields and grounding schemes, could function at levels associated with low-level testing but be damaged at higher levels. The test conditions provide confidence in the survival of the aircraft against all but severe lightning strikes.

The principal advantage of this test method is that the amount of scaling or extrapolation is not very great. Careful interpretation of the test data is necessary in order to provide confidence in an aircraft survival of severe lightning strikes. However, there is greater confidence in scaling factors of five to ten (from 20 or 40 kA to 200 kA) than factors of 200 required for the low-level pulse method. The data analysis must of course include interpretations of the measurements to validate the measurement process. The data analysis effort is much simpler and more readily accepted than the analysis required for lower level test methods.

### 4.2.4. Severe Full-Threat Pulse

Unfortunately, it is difficult or impossible to generate the severe lightning currents in large aircraft as can be demonstrated by a relatively simple analysis. The primary reason for this limitation is due to the inductance and resistance of the return circuit and the airplane. For an ideal conductor and the return circuit in a coaxial configuration, the test circuit surge impedance is typically 50 ohms. For 200 kA, this requires 1 MV to drive the test aircraft and 1.3 MV for the charge voltage of the pulser. These values are achievable but require specialized high voltage construction practices. For a large aircraft, the circuit impedance is more inductive. The inductance is approximately given by:

$$L = 120 \ln(h/2d)\, h/c$$

where h is the aircraft length, d is the aircraft diameter, c is the speed of light, and the units of the constant are henrys per second. For a 50-meter aircraft 3 meters in diameter, this results in an inductance of approximately 40 μhenrys. It requires 8 MV to drive 200 kA/μs into this inductance. Such a generator is not presently achievable. However, for a small general aviation size aircraft the inductance can be on the order of 3 to 4 μhenrys and only 600 to 800 kV is required to reach the 200 kA/μs rate-of-rise. While this is a large order for most general aviation manufacturers, such generators are well within the reach of several lightning test organizations.

### 4.2.5. Shock-Excited Pulse

The pulse techniques described above focus on directly attached current waveform simulation and associated EM fields. There is some concern that the high voltage and electric fields induced on an aircraft, just before a strike and during the aircraft charging, should also be considered in the simulation. The electric field mode can be simulated by using a spark gap between the aircraft and the pulse generator and between the generator and the ground. These spark gaps are to be placed at a structural extremity away from the pulser attachment. When the pulser is fired, the aircraft will be charged, through the pulser gap, toward the pulser voltage. The charging will be terminated when the aircraft-to-ground spark gap discharges to ground. This technique produces high voltage and electric field gradients on the aircraft to simulate the natural lightning effects.

This test method simulates the presence of corona, the leader attachment during the charging phase, and a return stroke as the aircraft discharges. The coupling mechanisms are more easily separated for analysis because the charging and discharging events are separate in time.

The major setup difference from prior techniques is that, in the shock-excitation test, the aircraft functions as the peaking capacitor. If the aircraft is isolated from ground, an additional peaking capacitor may be unnecessary. The discharge of the aircraft, when the output gap arcs over, should excite the internal circuits in much the same way as the discharge of an aircraft in a preionized lightning channel would when it is discharged by the return stroke.

Shock-excitation tests are unique because of the high-voltage aspects of the technique. The aircraft must be well isolated above ground. Specially designed high-voltage isolation pads placed under the wheels allow testing up to 400 kV on most aircraft.

A shielded high-voltage impulse generator is used as the excitation source. This shielding is required so that a clean output voltage waveform may be applied to the vehicle. To simulate the natural lightning charging and discharging of the aircraft, it is desirable to charge the aircraft to over one million volts with respect to the coaxially arranged return lines. At these voltages, realistic corona should be developed so that, when the aircraft discharges to ground, the transients produced will be representative of natural lightning. Essential elements of the test are fiber-optic data links which allow system transients to be monitored while the system is charged to very high voltages.

An important result of the shock excited test investigation (Clifford, Crouch, and Schulte, 1982) was that capacitive coupling (C dV/dt) was found to be the dominant coupling mechanism in some very important cases. In particular, the transients on high-impedance signal circuits used for single-wire computer logic circuit interconnections were found to be dominated by capacitive coupling. The situation is reversed for low-impedance circuits where inductive (L dI/dt) coupling dominates.

For these tests, the maximum values of the lightning parameters of interest (I, dI/dt, E, and dE/dt) are determined by the amount of charge stored on the aircraft before discharge occurs.

The major implication of these results for simulation testing is that sufficiently high voltages and rates of change of voltage must be present in the test to reproduce the natural lightning conditions. Since nonlinear corona and streamering effects are expected to play a role in the induced voltages and currents experienced by an aircraft struck by lightning, testing with low voltages (grounded vehicles) may not yield an accurate simulation.

The amplitude and duration of the oscillatory currents produced on the structure by the rapid discharge of the aircraft to ground (free response) are controlled by the dissipation factors in the test setup. These factors include arc impedance and corona streamering effects. When the test article is grounded, neither of these dissipation factors is present. It still remains to determine exactly what the correct values for the dissipation factors are, but additional laboratory studies, coupled with forthcoming flight data, should resolve those uncertainties.

### 4.2.6. Comparison of Test Methods

In a comparison of lightning simulation techniques on a composite test article (Cooley and Shortess, 1987), it was found that mean values of predicted currents due to severe lightning strikes for different techniques compared as follows:

| | |
|---|---|
| • low-level swept CW | +6 to +8 dB |
| • low-level pulse | -1 to -5 dB |
| • moderate-level pulse | baseline |
| • shock-excitation | +2 to +6 dB |

The moderate-level pulse results were used as a baseline. These data were considered more accurate than data measured using other techniques for the following reasons:

- The scaling factor from 7 kA to 200 kA had less uncertainty than for low levels of injected current.

- Non-linear effects were noted at several test points. Non-linear effects were not in evidence for the low-level tests.

- The spectral content was similar to the SAE-AE4L defined threat, Component A This allowed a minimal amount of analysis because a determination of resistive or dI/dt response was not necessary.

The CW predictions were larger (by a factor of two) and therefore more conservative than the predictions resulting from the moderate-level pulse tests. The low-level pulse results predicted responses about 1.5 times less than the moderate-level pulse. Shock-excitation was also a factor of two more conservative than the moderate-level pulse results.

### 4.2.7. Return Circuit Configuration

The return circuit for the lightning simulator and test article determines the field distribution around the object under test. More uniform field, voltage, and current distributions are produced by configuring the test article and return circuit as a coaxial transmission line, see figure 4.2-5. The electric and magnetic fields around the test object approximate field distributions for an aircraft in free space. An additional benefit is that this arrangement provides low circuit inductance and resistance which is required by some pulsers to produce a satisfactory waveform. This is particularly true for the RLC pulse generators.

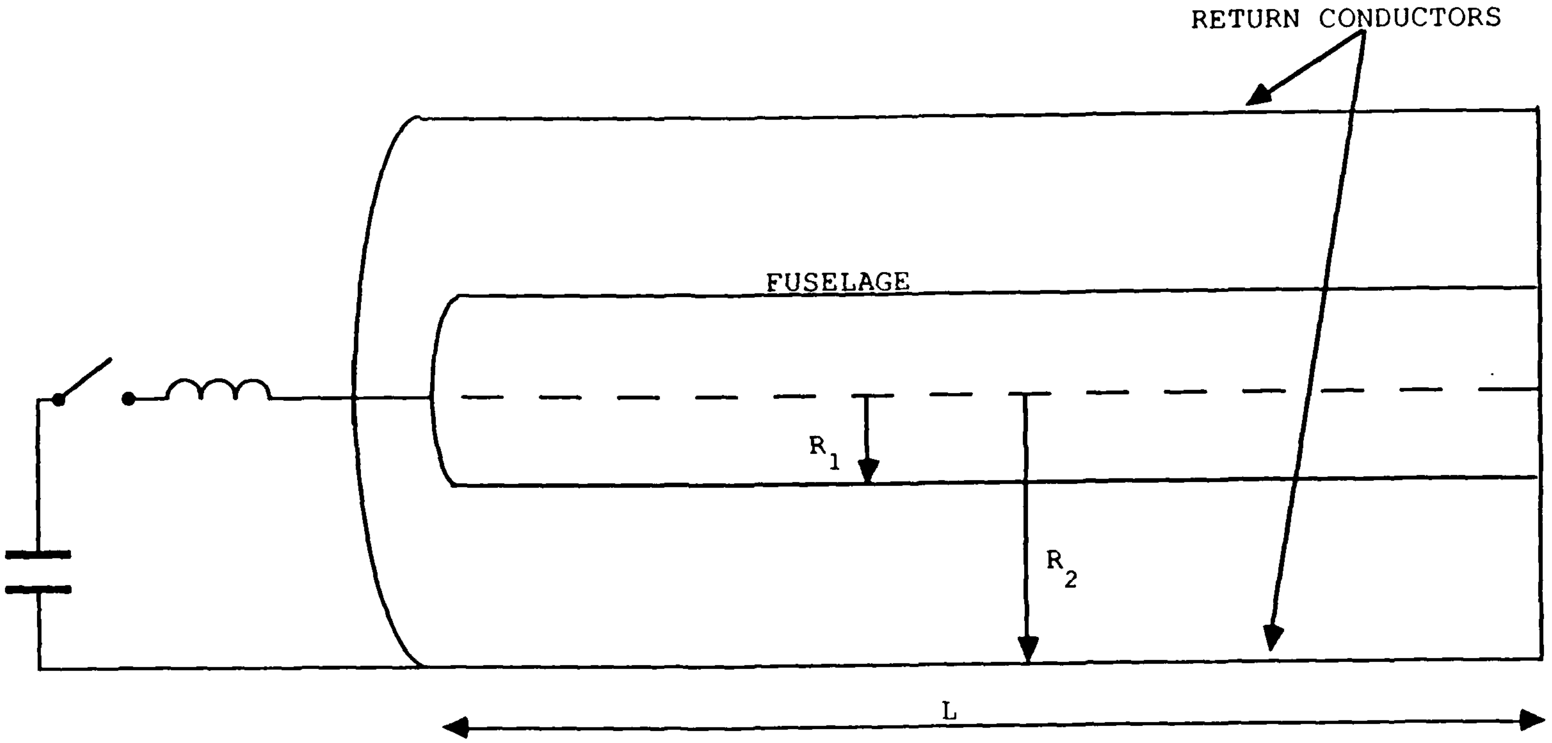
Some special considerations must be given for the construction of a return circuit. For high-level testing, the return circuit must sustain high currents and withstand high voltages. The return circuit must be made of a low resistance material, such as wire mesh or solid sheet, and maintain good physical contact to be suitable for low-level testing. The attachment points must be low inductance, have a high current carrying capability, and shield the test object from the fields of the pulser switch. The configuration should be built to accommodate all test configurations, e.g., nose-totail and wing-to-tail current injection. The construction should be such that the spacing between the return circuit and the test object maintains a constant impedance transmission line and any changes in return circuit geometry should be gradual compared to a wavelength of the highest frequency of interest. This is essential to prevent reflections due to impedance mismatches.

## 4.3. Data Quality Verification

Several recommendations are given in this section and can be used to assure that measured data is of high quality and is valid. These recommendations can be utilized for both CW and pulse tests.

Fiber optics should be used in both drive and signal transmission, if possible. The optics electrically isolate equipment to prevent ground loop currents. The data acquisition equipment should be placed in a screen room to provide shielding from pulser fields and to eliminate noise pickup. Pulser noise can be a major concern at high levels of current.

System calibrations must be performed daily to verify the correct operation of the CW measurement equipment and to obtain inherent system responses for proper data calibration. The measurements should be verified twice daily or at any time the system configuration changes. The data obtained from system calibrations are then subtracted from measurement data to remove inherent system responses. Calibration of some fiber optic units is necessary to define the amplitude of a known signal into a digitizer.



SIMPLIFIED AIRCRAFT GEOMETRY - THE AIRCRAFT FUSELAGE IS SHOWN AS A CYLINDER $R_1$ METERS IN RADIUS, L METERS LONG WITH RETURN CONDUCTORS SPACED AT AN EQUIVALENT RADIUS OF $R_2$ METERS.

FIGURE 4.2-5. SIMPLIFIED RETURN CIRCUIT

Noise measurements should be taken at each measurement location in each test configuration. The sensors are either a coaxial cable terminated in 50 ohms or a current probe with nothing through its center near test wiring as input to the fiber optics. These measurements can then be compared to the corresponding test point measurement to determine the signal-to-noise ratio. This is much easier to do in the frequency domain; however, a reasonable judgement can be made for a time domain measurement. A signal level 10 dB above the noise level is considered reliable data. Examples are shown in figures 4.3-1 and 4.3-2 of signal and noise measurements at the same location for CW and pulse tests.

End-to-end resistance measurements of the test setup should be made before and after each test configuration. This will be a measure of how well structural connectivity (joints, etc.) is maintained after the injection of current. An ohmmeter capable of accurately measuring a milliohm is necessary equipment for this check.

The input current should be monitored for every measurement. This current is used as a reference measurement during CW testing. During pulse testing, the input current must be checked to ensure proper pulser operation. The pulse amplitude will vary with each shot and should be recorded in the case of large variations. Data must be taken not only to characterize the simulator performance, but also to characterize the interaction and coupling of the simulated lightning environment with the test aircraft and the coupling effects on electronic/electrical systems.

Questionable current measurements can be checked in the following manner. With the current probe reversed, repeat the measurement and check the signal polarity. If the signal doe. not change polarity, then noise is being measured.

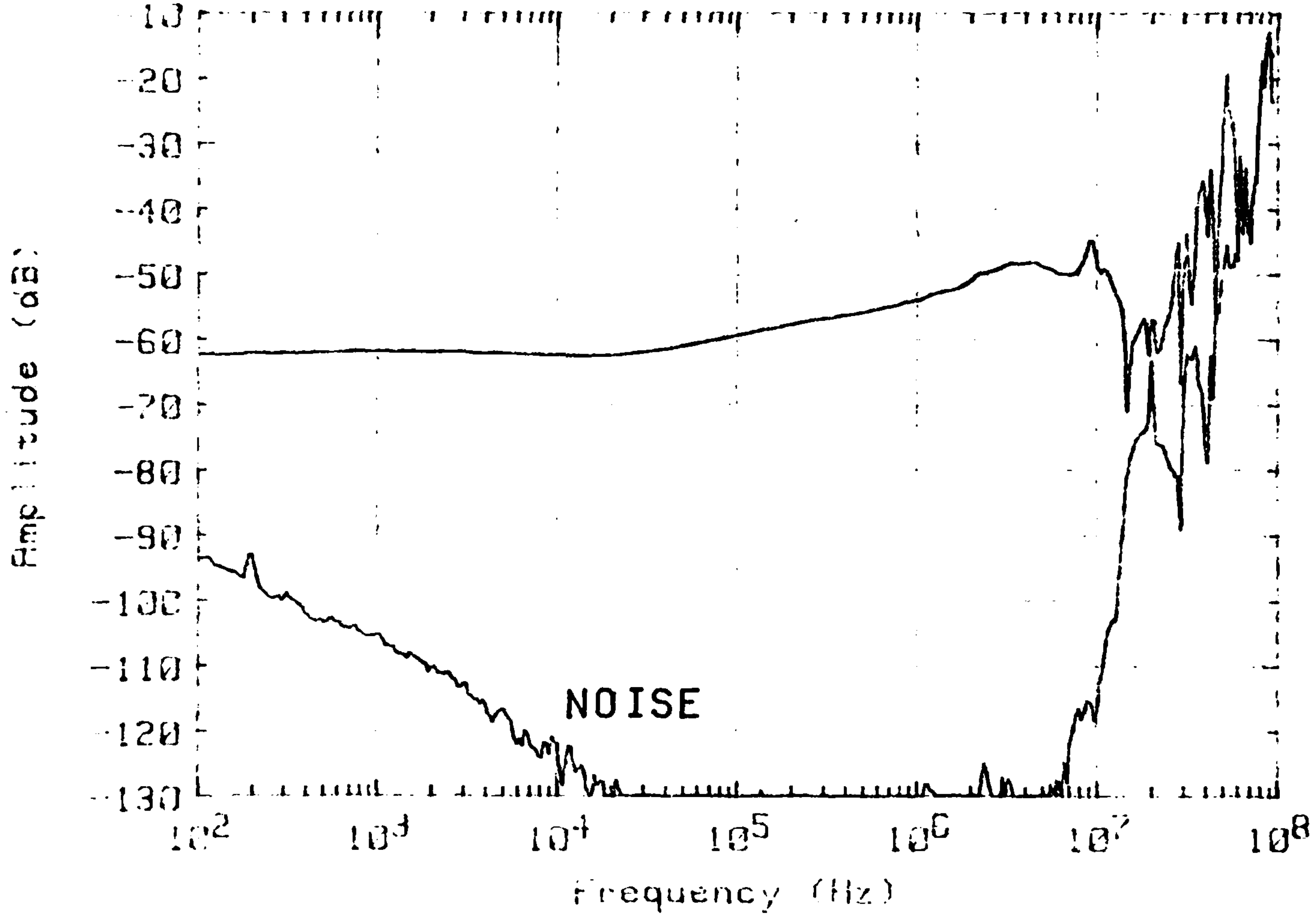
Validity checks should be performed by the experimenter during each test. These checks consist of comparing measured responses against theoretical models for their behavior to make sure the measured response curves are "reasonable." Any failure to produce "reasonable" data should be considered a failure in the instrument setup and/or test connections, and steps should be taken to correct the problem.

When using digital recorders, a vertical resolution should be set to obtain the measured response with the peak at least one-third of full scale to achieve adequate resolution of the signal response and to utilize the maximum bandwidth capabilities of the digitizer.

4.4. Bench Tests

Bench tests are used to test the susceptibility of individual components or subsystems to predicted levels. These predictions are based on measured data or analytic models for currents and fields at the location where the equipment would be installed.

Voltage and current transients induced in interconnecting wiring may be resistive, following the double exponential lightning source; a derivative, dI/dt, of the excitation source; or oscillatory, due to excitation of cable resonances.



TEST ID. No.: 3V2N
(8-12-85):COMPARISON OF SIGNAL TO NOISE AT THE SAME LOCATION

FIGURE 4.3-1. COMPARISON OF SIGNAL AND NOISE IN THE FREQUENCY DOMAIN

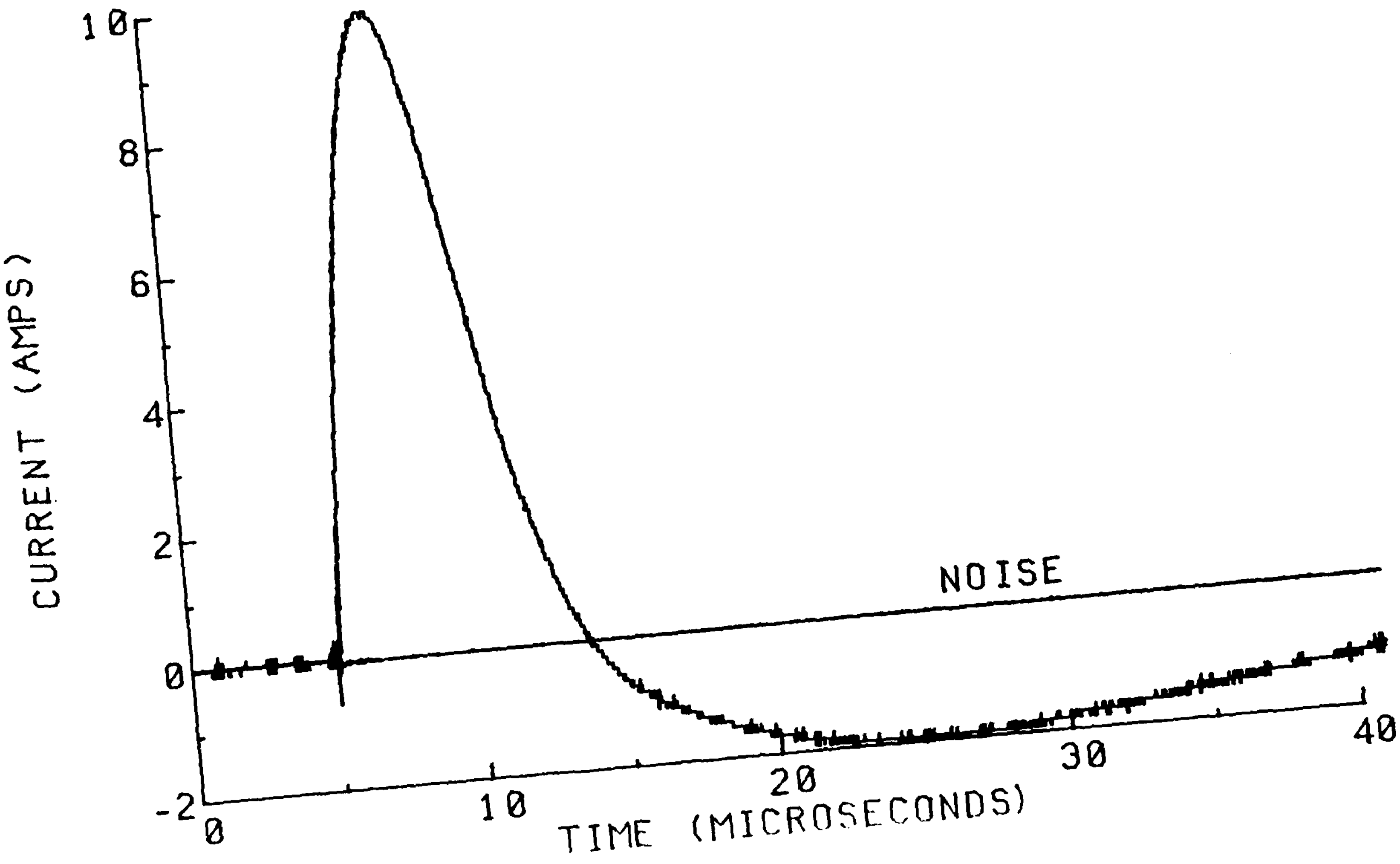


FIGURE 4.3-2. COMPARISON OF SIGNAL AND NOISE IN THE TIME DOMAIN

Waveforms, which define these responses, are shown in figure 4.4-1 (AC 20-53). These waveforms also represent the threat imposed on equipment at the cable interfaces.

Currents are injected into interconnecting cables by magnetic coupling using a clamp-on current transformer. Alternatively, electric and magnetic fields are injected into cables and enclosures by a parallel plate transmission line excited by a high current pulser. Power system transients are induced by direct series connection of a coupling capacitor and pulse generator across the power supply. A typical bench test setup for current injection is shown in figure 4.4-2.

Equipment is connected via appropriate cabling to simulate actual installed configurations. During the pulsing, the equipment is powered up and in an operational mode to simulate in-flight conditions. Equipment is monitored for damage or upset throughout the test sequence.

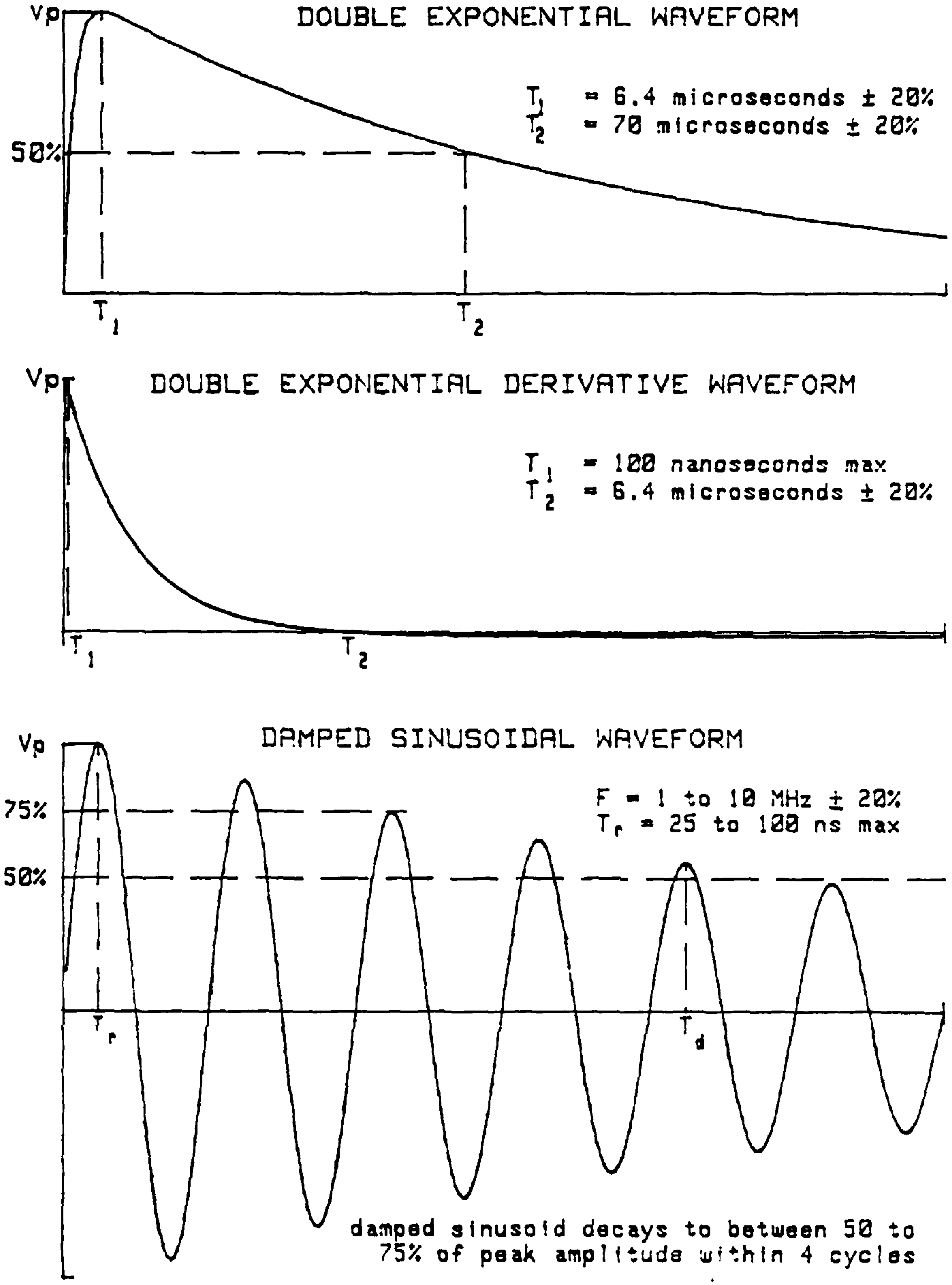
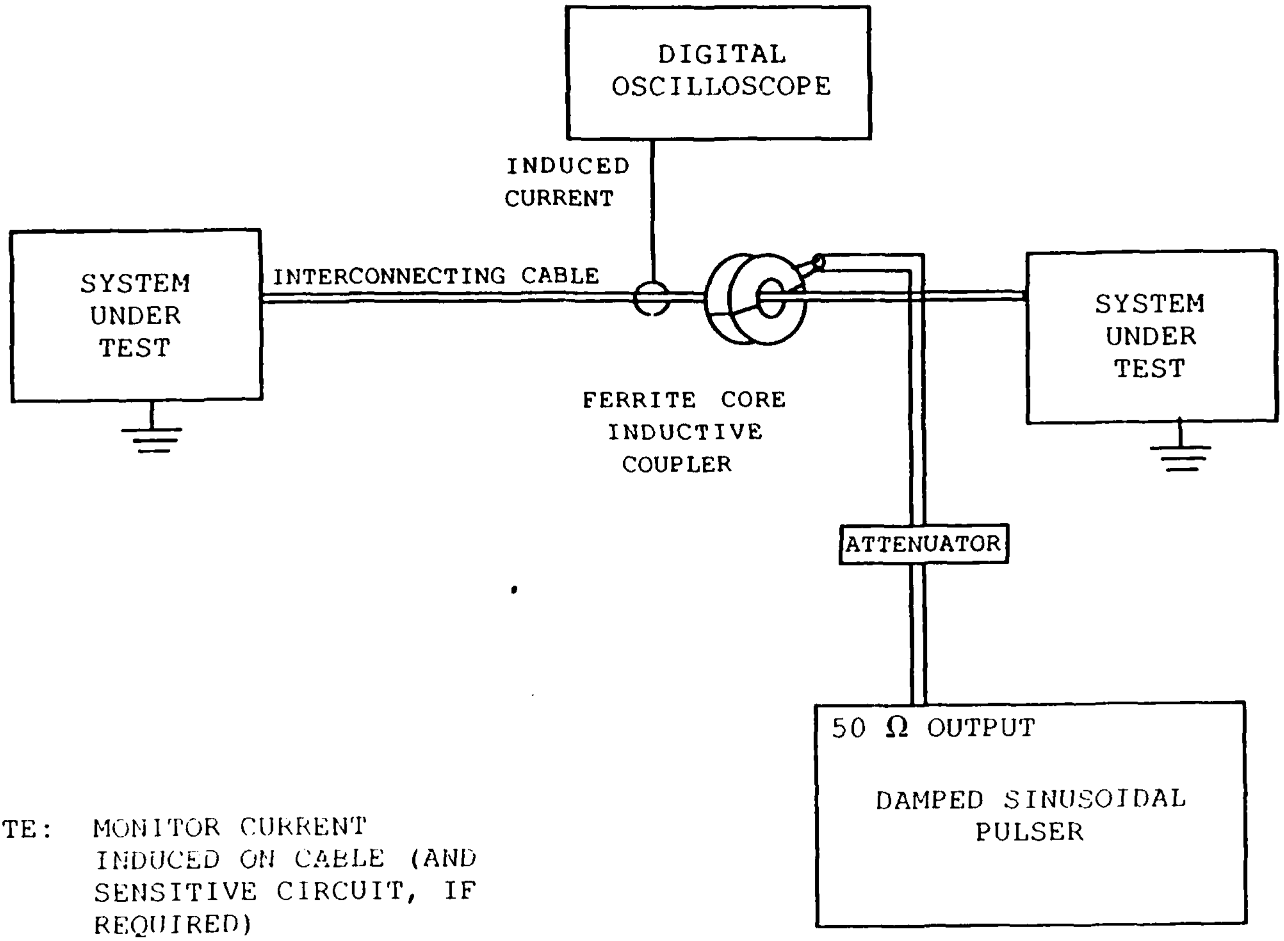


FIGURE 4.4-1. IDEAL BENCH TEST WAVEFORMS



NOTE: MONITOR CURRENT INDUCED ON CABLE (AND SENSITIVE CIRCUIT, IF REQUIRED)

FIGURE 4.4-2. CABLE CURRENT INJECTION TEST CONFIGURATION

# 5. INDIRECT EFFECTS PROTECTION - ANALYSIS TECHNIQUES

Accurately predicting the coupling of lightning to equipment within a structure such as an aircraft is a complex process. Figure 5-1 illustrates the principal elements of EM coupling prediction for lightning indirect effects. These elements follow the flow of energy from external environments to internal equipment.

The external coupling region contains resistive and inductive terms. The early time, inductive term appears as magnetic fields around the aircraft. These fields will build up and change rapidly in accordance with the lightning current pulses. The late time, resistive term appears as a voltage along the structure. While both terms are always present, the relative size of each depends upon the lightning pulse shape.

The internal fields present depend on several factors: penetrations through apertures, antennas, external wiring, and joints; diffusion through the skin; shape factors; and intrinsic shielding provided by the structure materials. External EM fields will leak into the interior of the aircraft through openings in the structure such as windows, radomes, access panels, and doors. Electrical imperfections such as joints, gaps, and holes also allow the entry of some EM fields. In addition to the EM field coupling, there may be resistive voltage drops in the structure as lightning currents flow. Currents may also flow inside the structure as a result of structural interconnections which can affect the internal EM environment. Leakage through apertures contributes to fast rise voltages. Effects due to diffusion through the skin will have a slow rise time compared to lightning pulses. Diffusion effects become important at frequencies where the structure thickness is equivalent to or greater than an electrical skin depth of the material.

Sources of internal currents in the wiring include B-dot coupling, E-dot coupling, and resistive voltage drop (IR) coupling. The magnitude of these sources is dependent on local structure, currents, and fields coupled to the interior.

Voltages are coupled into aircraft wiring in several ways. If part of a circuit connecting electronic equipment connects to structure, there will be a voltage difference between the wires and the structure. Voltages are also coupled between wires by electric and magnetic induction, even if the wires are not connected to the structure. The effects of induction depend upon the time rates of change of the lightning currents and EM fields. Since the total structural voltage drop depends upon both the inductive and resistive terms, voltages in the wiring depend upon the lightning current time rate of change as well as the peak current values.

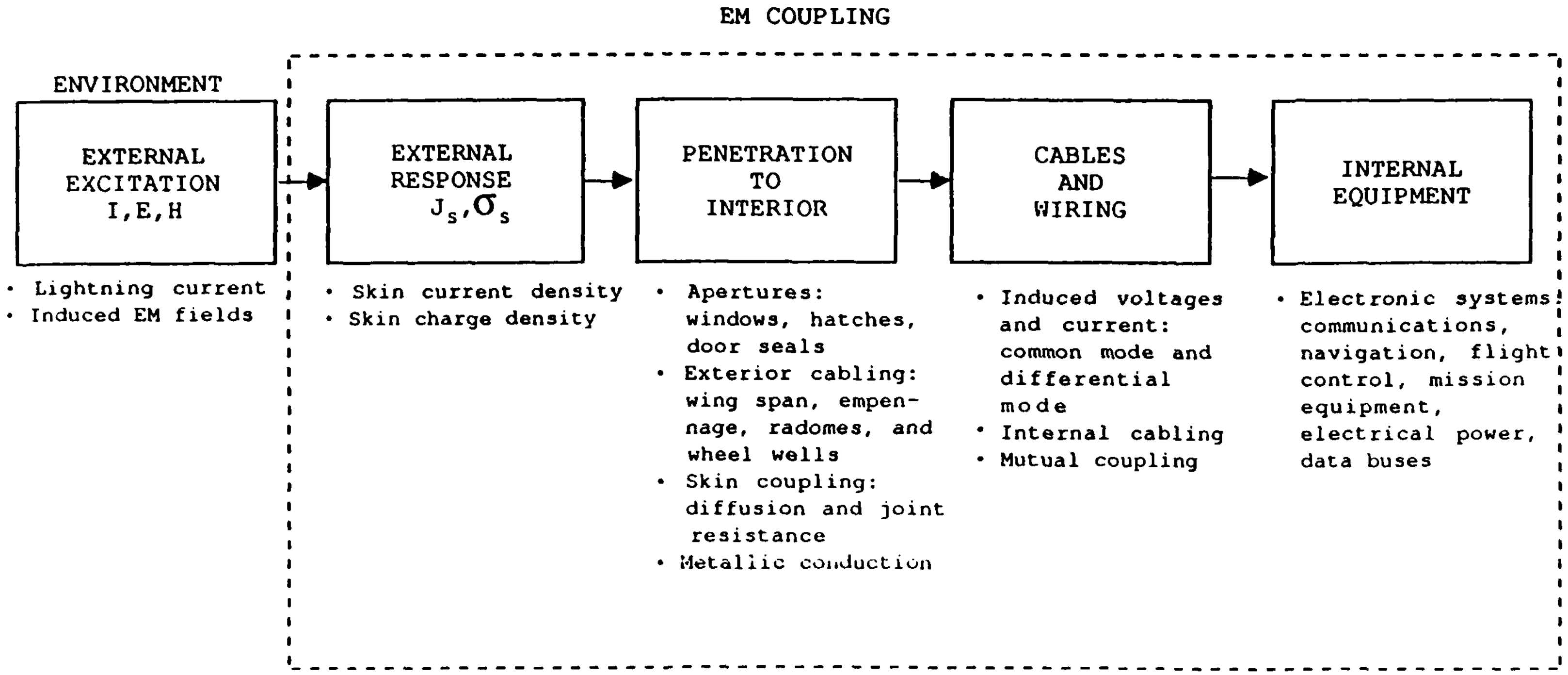

EM COUPLING
ENVIRONMENT
EXTERNAL EXCITATION I,E,H
• Lightning current
• Induced EM fields
EXTERNAL RESPONSE $J_s, \sigma_s$
• Skin current density
• Skin charge density
PENETRATION TO INTERIOR
• Apertures: windows, hatches, door seals
• Exterior cabling: wing span, empennage, radomes, and wheel wells
• Skin coupling: diffusion and joint resistance
• Metallic conduction
CABLES AND WIRING
• Induced voltages and current: common mode and differential mode
• Internal cabling
• Mutual coupling
INTERNAL EQUIPMENT
• Electronic systems communications, navigation, flight control, mission equipment, electrical power, data buses

FIGURE 5-1. ELEMENTS OF EM MODELING AND ANALYSIS FOR LIGHTNING INDIRECT EFFECTS

For an aircraft made of aluminum, the coupled voltages are rarely important except when the lightning current flows through joints and hinges. However, the resistance of an advanced structural material such as G/E is many times that of aluminum. Voltages of a few tenths of a volt have no effect in an aluminum structure. Voltages that are larger by a factor of several hundred to a thousand times than those for aluminum, because of the lower conductivity of the composite materials can become very serious.

Coupling to electronic equipment is dependent on the termination and source impedances, the circuit configuration, and the wire bundles which connect to each box.

### 5.1. Modeling Methods for Composite Structures

In advanced technology aircraft, EM coupling models for lightning protection design must account for the composite structural materials and the fastener joining techniques. Many of the present models (such as the environment, external response, cable and wiring, and internal equipment) used for metal aircraft are useful for composites. The penetration to interior models require changes for particular aircraft and wiring configurations.

The modeling of energy penetration from the exterior to the interior has several common elements for any aircraft particularly in the apertures and exterior wiring and cables. The principal difference between metal and composite aircraft lies in the increased contribution of the IR in the fuselage and wing skins and in the increased current flow paths in the structure. The G/E structure has typically 1000-3000 times higher resistance than the similar aluminum metal structure. This higher resistance leads to strong interactions between the external and internal EM regions for composite structures.

For frequencies above a few megahertz, or for early time (i.e, on the order of a few microseconds), there is no difference in the lightning response between aluminum and graphite structures. This is because at high frequencies, the EM "skin effect" forces the currents to the outside of materials, to outside surfaces, and to sharp radius of curvature portions of the structure. Protection against the early pulse is essentially the same for both structural materials. Wiring must be kept near metallic structure to reduce the magnetic field B-dot coupling factors.

The main difference in energy penetration between graphite and aluminum structures is in the frequencies below the megahertz range, or for late time (i.e., on the order of a few tens of microseconds). For this range of frequencies, considerable current flows into the interior as a result of the range of thicknesses and materials used in aircraft structure. Since the current flow is resistive for G/E materials, the protection measure of keeping the wiring close to the structure will not have any protective effect. Furthermore, the IR voltage drop will be much larger for G/E than for aluminum.

## 5.2. Computer Modeling Codes

Analytic models are useful tools in determining the effectiveness of various protection designs. Analytic models can be used in parallel with testing to validate test results or to assess various protection methods for use on particular equipment.

There is no single analytic method which can provide accurate results at all levels of EM coupling, from lightning interaction with an aircraft to transients in the wiring. A multi-level analysis, as shown in figure 5.2-1, can be used to provide answers to the overall coupling problem. Using this approach, the exterior currents on the airframe due to a lightning strike are calculated first. Next, the interior fields and shield currents are calculated. These are determined by penetrations due to joints, apertures, and diffusion. The final level of analysis is to compute the transients at the component level. The input currents to each level are those calculated from the preceding level.

This type of analysis assumes that the coupling between levels is negligible. This implies that metal structure or wiring inside the aircraft does not significantly affect the exterior skin currents. This assumption is not valid for an aircraft consisting of mainly G/E skin. In this case, internal metal structure will carry the bulk of the current at low frequencies. Internal fields will be dominated by these currents rather than diffusion through the composite material. Models of mixed materials aircraft need to include internal structure in the external coupling model to accurately model current flow through the aircraft.

A description of some of the various computer codes available, their limitations, and the type of analysis to which they are suited is given below. Table 5.2-1 summarizes the capabilities of each program. The User's Manual for AC 20-53 gives additional details and references for some of these codes.

Surface currents have been calculated using finite difference time domain and method-of-moments techniques. Method-of-moment codes use a wire grid, surface patches, or strips to model the vehicle surface.

WIRANT, Numerical Electromagnetics Code (NEC), General Electromagnetic Model for the Analysis of Complex Systems (GEMACS), REDIST, THREDE, T3DFD, Thin Wire Time Domain (TWTD), Lumped Parameter Network (LPN), and transmission line models have all been used to determine surface currents. Care must be taken in the model definition to provide valid results.

WIRANT is a wire grid method-of-moments code which can be run on an IBM-XT or compatible personal computer, or a mainframe computer. The calculated currents and fields are output in the frequency domain. The code handles a frequency range which is suitable for lightning. It has been used to model several aircraft, e.g., Boeing 757, to determine EM coupling due to lightning. Results have compared favorably with experimental data. Plane wave excitation or current injection may be used to drive the models. Mixed materials may be incorporated into these models.

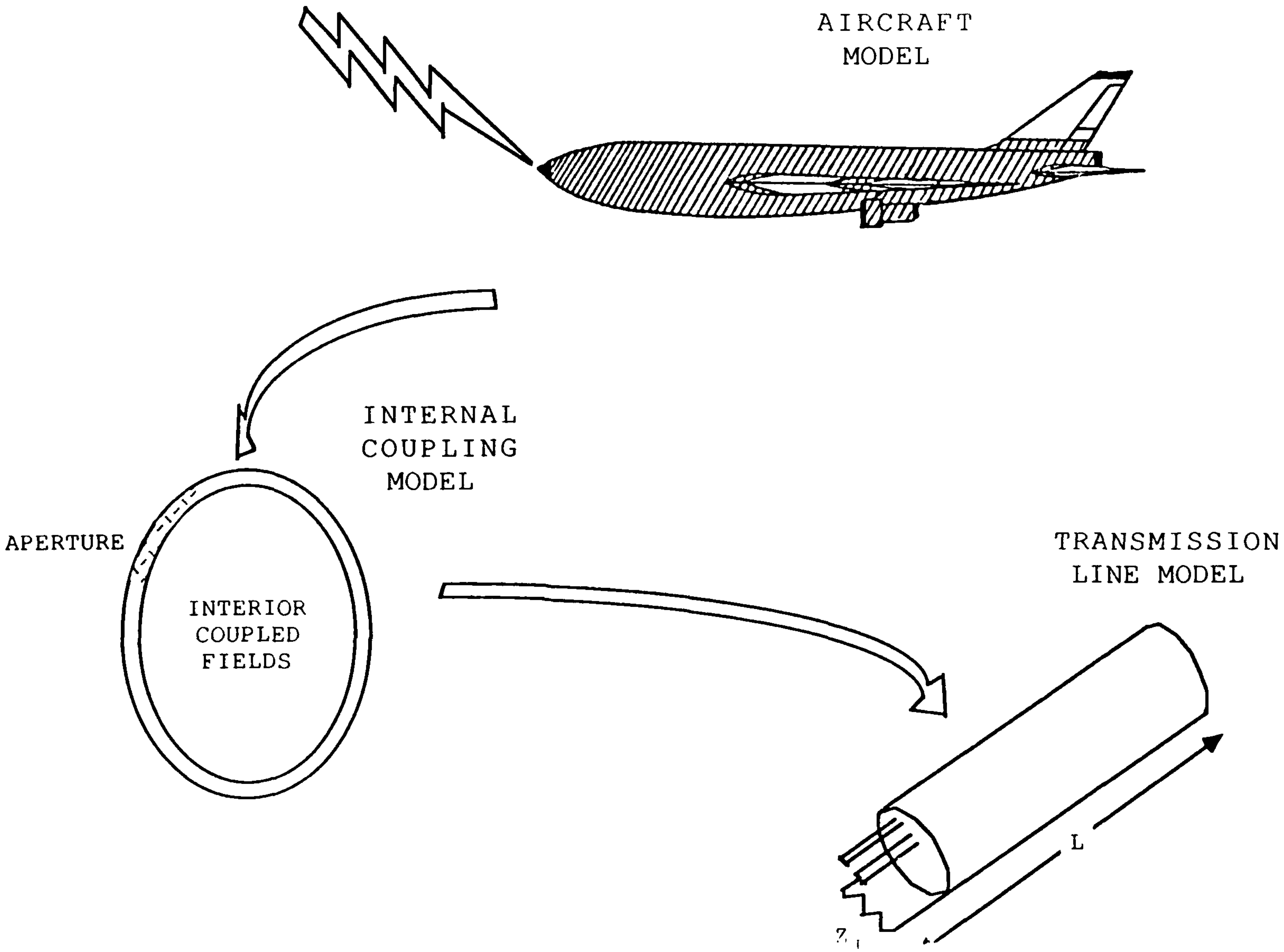


FIGURE 5.2-1. MULTILEVEL LIGHTNING COUPLING ANALYSIS APPROACH

TABLE 5.2-1. CAPABILITIES OF COMPUTER CODES FOR MODELING EM COUPLING TO AIRCRAFT

| | COMPUTER CODE | LIGHTNING THREAT | EXTERNAL COUPLING $J_s$, $\sigma_s$ | INTERNAL COUPLING (APERTURES & DIFFUSION) | CABLE PENETRATION (SHIELDS & BUNDLES) | INTERNAL WIRING | PIN TRANSIENTS | EQUIPMENT UPSET |
|---|---|---|---|---|---|---|---|---|
| EXTERNAL MODELS | WIRANT | OK | OK | LIMITED SIZE | OK | N/A | N/A | N/A |
| | THREDE | OK | SHORT TIME | OK | N/A | N/A | N/A | N/A |
| | TRANSMISSION LINE | OK | OK | N/A | N/A | N/A | N/A | N/A |
| | GEMACS | OK | OK | OK | OK | OK | N/A | N/A |
| | T3DFD | OK | OK | OK | N/A | N/A | N/A | N/A |
| | NEC2 | OK | OK | N/A | N/A | N/A | N/A | N/A |
| | LPN | OK | OK | ESTIMATE | N/A | N/A | N/A | N/A |
| | TWTD | N/A | ESTIMATE RESONANCE | N/A | N/A | N/A | N/A | N/A |
| | RESISTOR | OK | LATE TIME | N/A | LATE TIME | N/A | N/A | N/A |
| | REDIST | OK | 2-D LIMITS | 2-D LIMITS | OK | OK | N/A | N/A |
| INTERNAL MODELS | SCEPTRE | N/A | ? | ? | OK | OK | OK | N/A |
| | SPICE | N/A | OK | N/A | OK | OK | OK | OK |
| | TRANSSIM | N/A | ? | ? | OK | OK | ? | N/A |
| | SINLINE | N/A | N/A | N/A | CABLE/WIRE | OK | ? | N/A |
| | TRAFFIC | N/A | N/A | N/A | CABLE/WIRE | OK | OK | N/A |
| PIN TRANSIENTS | HANAP | N/A | N/A | N/A | N/A | N/A | OK | OK |
| | TCAP | N/A | N/A | N/A | N/A | N/A | OK | OK |
| | CIRCUS | N/A | N/A | N/A | N/A | N/A | OK | OK |
| | SCORCH/ SUPERSAP | N/A | N/A | N/A | N/A | N/A | OK | N/A |

NEC is a method-of-moments code which uses segmentation by patches. The upper frequency limit is about 100 MHz. Both free space excitation and current injection can be modelled. This code requires a large amount of memory and can only be run on a mainframe computer.

GEMACS is a method-of-moments code which can also be run on an IBM-AT or mainframe computer. Predictions of external coupling to a model (segmented into a wire grid or patches), fields penetration due to aperture coupling, and the induced currents on a wire in a cavity behind the aperture can all be obtained. An example of the use of the code is given in Coffey and Hebert (1986). An entire session of the Applied Computational Electromagnetics Society (ACES) conference was devoted to the capabilities of this code (1988).

REDIST is a two-dimensional method-of-moments code which utilizes thin strips to form models. This code was developed on an IBM-XT compatible personal computer. It provides frequency domain currents and fields, both external and internal, and can be used for mixed material structures. Coupling to wiring can also be determined with this code. Limitations arise where the structural cross-section changes rapidly and when the structure thickness is greater than a skin depth of the material. Verification using scale models has provided good agreement (Geren, Melander, and Hall, 1987). Results have been compared to experimental data from a composite test bed aircraft (Cooley and Shortess, 1987).

THREDE is a three-dimensional finite difference computer code which runs on a mainframe computer. The primary limitation of this code for application to lightning is that most of the Low Frequency (LF) response is not included in the time domain response calculated by the code. Since a dominant coupling mechanism for composite structures is late time (after several microseconds) resistive drops in the structure, this code would not be suitable for modelling mixed material aircraft.

T3DFD is similar to THREDE, but allows mixed skin conductivities within the model.

TWTD utilizes a thin wire approximation and gives solutions in the time domain. It provides quick approximations of aircraft resonances. The code cannot treat current injection and so is not applicable to lightning.

LPN codes model physical structures with an equivalent circuit. This has the advantage of simple development and implementation. Much less memory is required for these simpler models. Currents can be determined by using a transmission line code. LPN theory may be applied to internal coupling provided calculations of the external coupling are available to be used as input to the internal model.

Transmission line models are useful to provide resonances and current densities. These models are usually simpler than models using a wire grid code. The SAE AE4L Orange Book and Simpson and Katzer (1988) give examples of the use of this type of code. Transmission line theory is applicable at all levels of coupling analysis.

Resistor models can be used to determine late time responses, due to structural IR drops, with fair accuracy. An example of this very simple model is given in section 6.2. Internal structure and cable bundles can be included. The resistance can be easily calculated by known physical parameters or measured values. Cooley and Shortess (1987) contains another example of this type of modelling.

TRAFFIC, SINLINE, SCEPTRE, TRANSSIM, and SPICE may be used in conjunction with results obtained from one of the codes described above which calculates external coupling to determine transients on internal wiring. TRAFFIC consists of a library of codes and is a part of PRESTO (see PRESTO User's Guide). It provides frequency domain output for wiring transients. SPICE and SCEPTRE are time domain codes and can thus include non-linear elements.

HANAP calculates pin transients in the frequency domain and design margins using a mainframe computer. Threshold Circuit Analysis Program (TCAP) can perform similar calculations for simple circuits on a hand calculator (Pryzby and Plumer, 1984). For non-linear analysis, CIRCUS, a code within the TRAFFIC library, will calculate desgin margins. SCORCH and its predecessor, SUPERSAP, may be available as a commercial product to calculate pin transients.

# 6. SUPPLEMENTAL EXAMPLES

## 6.1. Coupling to Wiring

An example of a simple two-dimensional model is used to illustrate coupling to wiring within a mixed materials structure. The model, shown in figure 6.1-1, is a box which has three metal sides and one G/E side. The conductivity and thickness of each side is indicated on the figure. The thicknesses used are for typical aircraft structure. The code RESIST was used to evaluate this model.

Numbers 1 through 6 inside the box indicate the shield locations evaluated. Each model run contained a single wire at a different location. The output was given as a transfer function of the shield current relative to the input current for the entire structure. Figure 6.1-2 contains the transfer functions for each shield location.

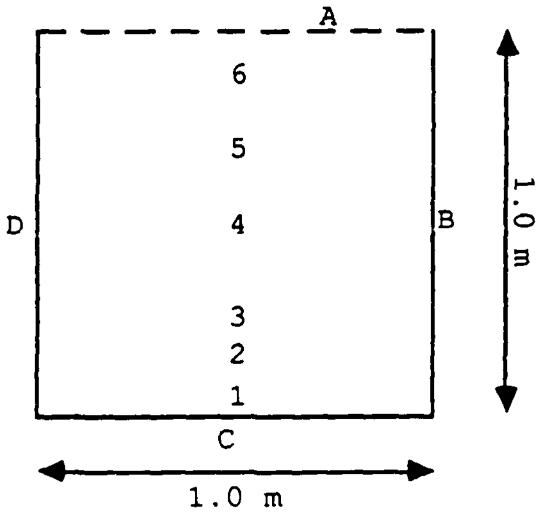
A worst case estimate of shield currents can be obtained by multiplying the calculated shield transfer function by the threat, in this case a double exponential lightning spectrum, and Fourier transforming the resultant spectrum to the time domain. Current pulse responses for each shield location are shown in figure 6.1-3. The peak currents vary by an order of magnitude. Induced shield currents are small for locations near the metal bottom of the box and increase steadily as the shield is moved toward the graphite lid.

These estimates of current represent worst case (upper bound) strikes, because the entire 200,000 A is assumed to flow through the box and shield. This would not be the case if the box were part of an aircraft. In order to obtain a more realistic estimate of internal shield currents, a vehicle external model must be analyzed to obtain the division of current between the modeled box and the remainder of the vehicle. This transfer function is then multiplied by the shield transfer function (calculated previously) and the lightning threat to obtain the shield current relative to the aircraft current.

Leakage through the graphite can be illustrated by looking at the magnetic fields calculated with this model. Figures 6.1-4 and 6.1-5 show magnetic field contour lines for the box at 1 kHz and 1 MHz. At 1 kHz, the G/E is transparent to the fields. The fields are excluded from the box at higher frequencies due to the skin effect. This indicates why early time responses for graphite or metal structures are similar.

After determining the shield currents, the current and voltage transients at the component level can be calculated using an appropriate method. A transmission line formulation is used here.

REDIST MODEL
METAL BOX WITH GRAPHITE LID



Shield locations denoted by numbers 1-6.

| WALL | STRUCTURAL PARAMETERS | |
|---|---|---|
| | THICKNESS<br>(m) | CONDUCTIVITY<br>(mhos/m) |
| A | 2.3E-3 | 1.5E4 |
| B | 1.3E-3 | 3.5E7 |
| C | 1.3E-3 | 3.5E7 |
| D | 1.3E-3 | 3.5E7 |
| SHIELD | 2.54E-4 | 3.5E7 |

FIGURE 6.1-1. REDIST EXAMPLE MODEL GEOMETRY

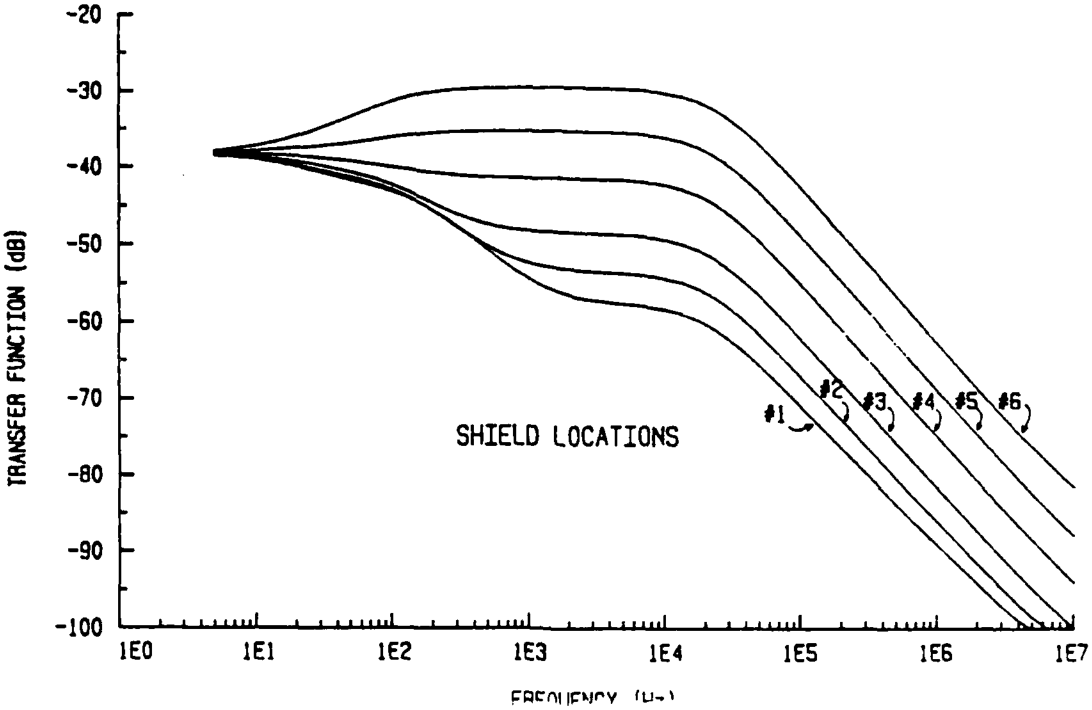


FIGURE 6.1-2. SHIELD TRANSFER FUNCTION FOR METAL/GE BOX FOR SEVERAL SHIELD LOCATIONS

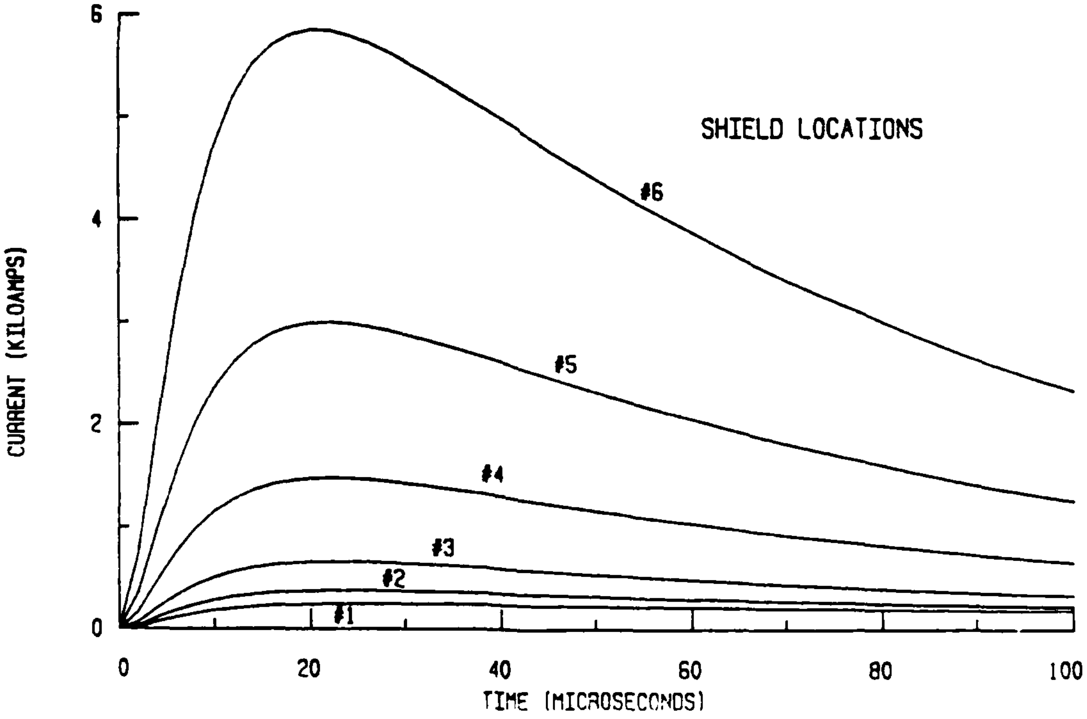


FIGURE 6.1-3. SHIELD CURRENT FOR METAL/GE BOX FOR SEVERAL SHIELD LOCATIONS FOR 200 kA ATTACHED LIGHTNING

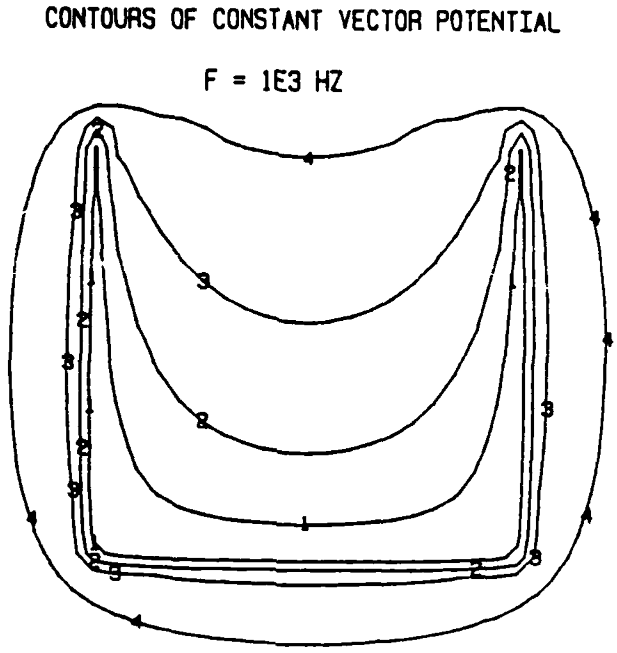


FIGURE 6.1-4. MAGNETIC FIELD CONTOURS FOR METAL/GE BOX AT 1 kHz

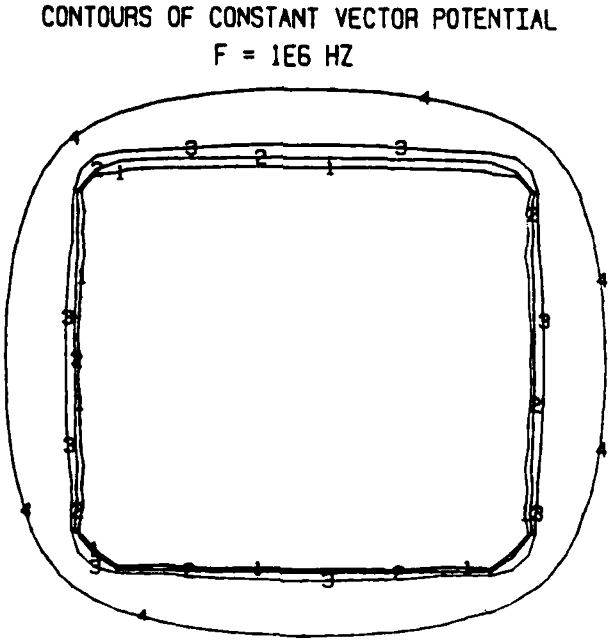


FIGURE 6.1-5. MAGNETIC FIELD CONTOURS FOR METAL/GE BOX AT 1 MHZ

The coupling to the shields is a continuous magnetic or electric field interaction along the length of the shield. This method of calculation uses a continuous voltage source term running the length of the transmission line model to the equipment terminations at each end. Basic assumptions made for this model are:

- The shield transfer function (voltage relative to current) is given by $R_{shield} + jw \times L_{shield}$

  where

  $R_{shield} = 1.78 \times 10^{-3}$ ohms per meter

  $L_{shield} = 8.96 \times 10^{-10}$ henrys per meter

  These numbers were obtained from measurements made on braided aluminum shields.

- The termination impedance was assumed to be 100 ohms at each end.

- The voltage and currents were calculated at one end of a transmission line with a continuous voltage source assumed equal to the shield current times the shield transfer function.

- The line length, L, was assumed to be 10 meters.

The results can be seen in figure 6.1-6. The time domain voltage waveforms for each of the six shield locations are shown. The peak voltages can be estimated using the following equation.

$$V_{peak} = V_{oc} / 2$$

$$= (I_{peak} \times R_{shield} \times L) / 2$$

where $V_{oc}$ is the open circuit voltage and $I_{peak}$ is the peak shield current.

For shield location #5 with a peak current of about 3 kA,

$$V_{peak} = (3 \text{ kA} \times 1.78 \times 10^{-3} \text{ ohms/m} \times 10 \text{ m}) / 2$$

$$= 26.7 \text{ V}$$

Larger voltages will be induced on longer cables and smaller voltages will be induced on shorter cables. This is due to resonance effects on the cables. Figure 6.1-7 illustrates the variation in induced voltages for several line lengths.

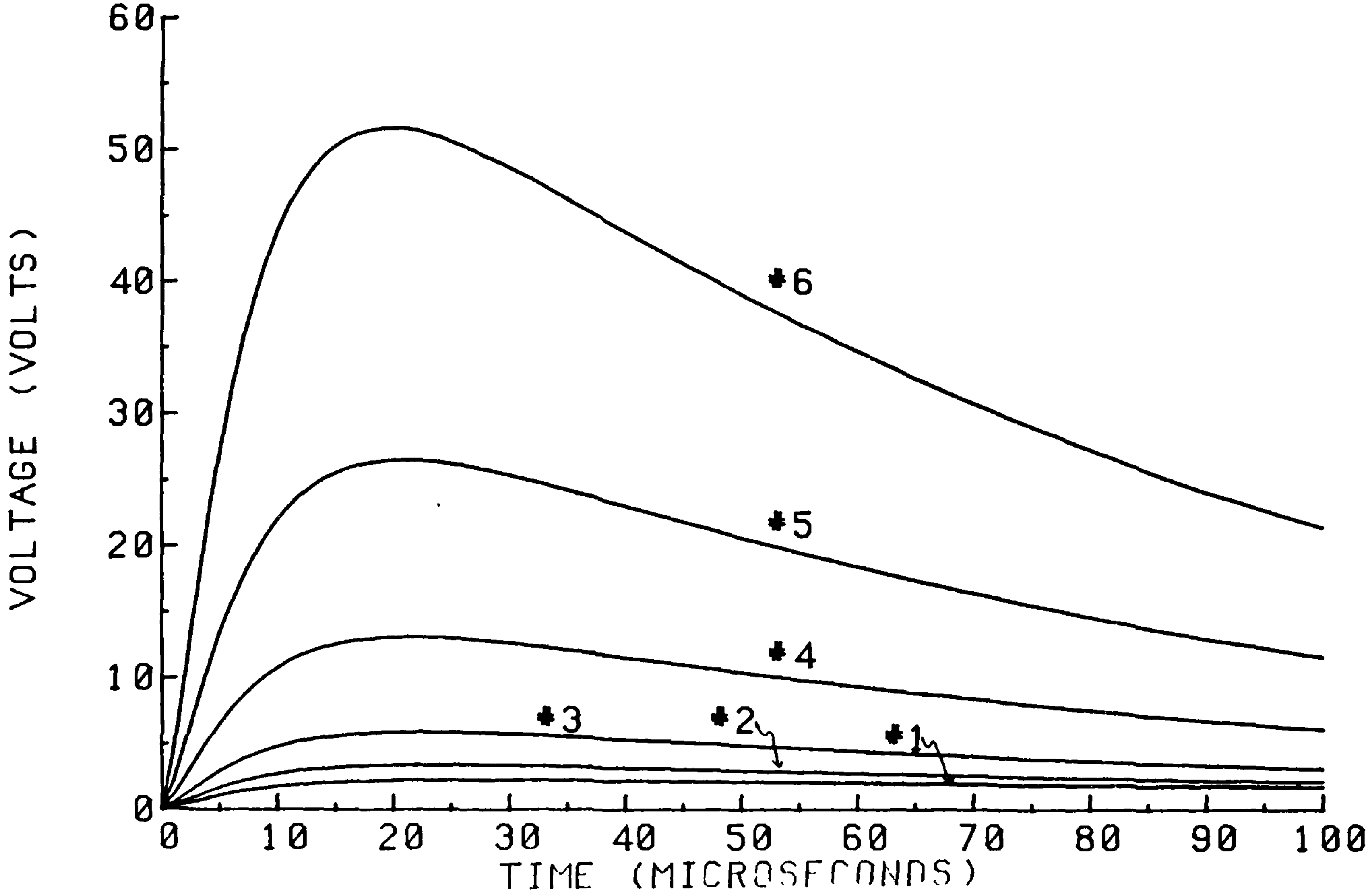


FIGURE 6.1-6. PIN VOLTAGE WAVEFORMS FOR SEVERAL SHIELD LOCATIONS

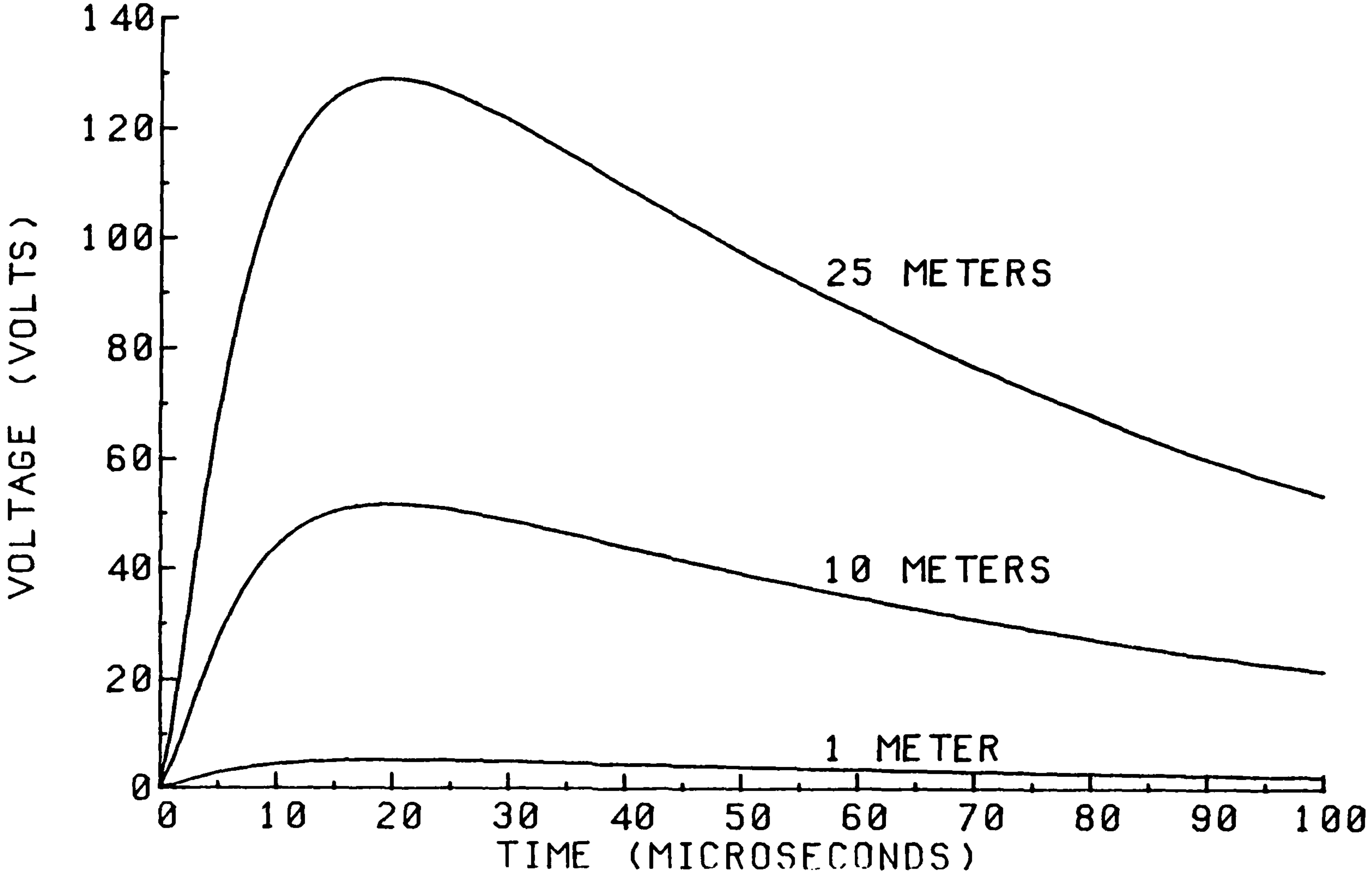


FIGURE 6.1-7. PIN VOLTAGE WAVEFORMS FOR SHIELD LOCATION #6 FOR VARIOUS LINE LENGTHS

## 6.2. Composite Wing Model

A dc resistance model of a composite wing used in NASA tests was constructed to determine the amount of current flowing through various sections of the wing. Results of this modeling study will predict energy flows into various structural members and fasteners. A dc model is appropriate for lightning studies since structural and fastener damage occurs because of the high energy levels. These high energy levels result primarily from large LF components of the lightning pulse.

An estimate of the dimensions and properties of the composite wing are listed in table 6.2-1. The spars were considered "I" beam sections 1/4 inch thick with the remaining values given in the table. The skin was taken as a product of average dimensions obtained from a NASA report, Pryzby and Plumer (1984). Both sides of the wing skin were considered in the total area. The braid running in the leading wing edge was assumed to be 1/2 inch braid which was taken to have 3 milliohm per meter resistance, as measured in previous studies. Fasteners were assumed to have a resistance of 10 milliohms each. These resistances are similar to predictions of various fastener resistances in Cooley (1985). The length of the wing is assumed to be 5.77 meters.

The structure resistance, $R_s$, is determined using the following equation.

$$R_s = L / (\sigma \times A)$$

where L is the length in meters, A is the area in square meters, and $\sigma$ is the conductivity in mhos (or siemens) per meter.

This simple resistance model predicts current level as percentages of total current in table 6.2-1. The predictions are obtained simply by resistive division between each item and the entire structure. These are compared to measured values for late time (80 microseconds) into the pulse. The agreement is good considering that dimensions, conductivities, number of fasteners, and fastener resistances are not accurately known.

TABLE 6.2-1. COMPOSITE WING RESISTANCE MODEL RESULTS VS. MEASUREMENTS

| ITEM | WIDTH (IN) | HEIGHT (IN) | AREA (IN$^2$) | CONDUCTIVITY (MHO/M) | STRUCTURE RESISTANCE (OHM) | TOTAL FASTENER RESISTANCE | STRUCTURE RESISTANCE W/FASTENERS | ITEM CURRENT (% OF TOTAL) | MEASURED CURRENT (3) (% OF TOTAL) |
|---|---|---|---|---|---|---|---|---|---|
| FRONT SPAR | 1.00 | 2.00 | 0.88 | 28000 | 0.363 | 0.005<br>(1) | 0.368 | 3.4 | 2% TO 5% |
| CENTER SPAR | 2.50 | 5.00 | 2.38 | 28000 | 0.134 | 0.005<br>(1) | 0.139 | 9.0 | 2% TO 5% |
| REAR SPAR | 1.50 | 3.00 | 1.38 | 28000 | 0.231 | 0.005<br>(1) | 0.236 | 5.3 | 2% TO 5% |
| SKIN | 77.00 | 0.0875 | 6.74 | 28000 | 0.047 | 0.001<br>(2) | 0.048 | 25.8 | 29% |
| BRAID | | | | | 0.017 | 0.005<br>(1) | 0.022 | 56.6 | 71% |

TOTAL RESISTANCE
OF STRUCTURE = 0.012 OHM

FASTENER RESISTANCE
ASSUMED = 0.01 OHM

(1) 2 FASTENERS ASSUMED
(2) 10 FASTENERS ASSUMED
(3) MEASURED DATA FROM PLUMER (1984)

## BIBLIOGRAPHY

AC 20-53 (Draft), Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning, 8 June 1988.

Applied Computational Electromagnetics Conference Proceedings, Session 7, Monterey, CA, March 1988.

Butters, W.G., et al., "Assessment of Lightning Simulation Test Techniques," Proceedings of IAGC on Lightning and Static Electricity, March 1982.

Clifford, D. W., K. E. Crouch, E. H. Schulte, "Lightning Simulation Testing," IEEE Transactions, EMC-24, V2, May 1982.

Coffey, E. L. and Lt. J. L. Hebert, "Implementation of GEMACS for Lightning Interaction Analysis," IAGC on Lightning and Static Electricity, June 1986.

Cooley, W. W., Determination of Electrical Properties of Grounding, Bonding, and Fastening Techniques for Composite Materials, Report No. DOT/FAA/CT-86/8, December 1985.

__________, and D. L. Shortess, Lightning Simulation Test Technique Evaluation, Report No. DOT/FAA/CT-87/38, November 1987.

Craft, W.L., Protection Optimization for Advanced Composite Structures, Grumman Aerospace Corporation, 1981.

Federal Aviation Administration - Florida Institute of Technology, Workshop on Grounding and Lightning Technology, March 1979.

Federal Aviation Administration - Georgia Institute of Technology, Workshop on Grounding and Lightning Protection, FAA-RD-78-83, May 1978.

Fisher, F. A. and J. A. Plumer, Lightning Protection of Aircraft, NASA Report RP-1008, 1977.

Geren, W. P., B. G. Melander, and D. L. Hall, "Lightning Current Redistribution," Applied Computational Electromagnetics Newsletter, Vol. 2, No. 1, May 1987.

IEEE Electromagnetic Compatibility Society, "Special Issue on Lightning and Its Interaction With Aircraft," IEEE Transactions on Electromagnetic Compatibility, Volume 24, No. 2, May 1982.

International Aerospace and Ground Conference on Lightning and Static Electricity, Dayton, OH, June 1986.

International Aerospace and Ground Conference on Lightning and Static Electricity, Fort Worth, Texas, June 1983.

International Aerospace and Ground Conference on Lightning and Static Electricity, Oklahoma City, OK, April 1988.

International Aerospace and Ground Conference on Lightning and Static Electricity, Orlando, FL, June 1984.

International Aerospace and Ground Conference on Lightning and Static Electricity, Oxford, FL, 1982.

Lightning Test Waveforms and Techniques for Aerospace Vehicles and Hardware, Report of Society of Automotive Engineers Committee AE4L, 20 June 1978.

Melander, B. G. and W. W. Cooley, Threat Environment Definition, D180-27423-1, The Boeing Company, February 1984.

MIL-B-5087B (ASG), Bonding, Electrical, and Lightning Protection, for Aerospace Systems, Amendment 2, 31 August 1970.

MIL-STD-1757, Lightning Qualification Test Techniques for Aerospace Vehicles and Hardware, 17 June 1980.

Mosher, J. and M. Wojtowicz, TCAP - Threshold Circuit Analysis Program Version 3.0 User's Guide (First Draft), TRW Report, August 1986.

Orange Book User's Manual - Lightning Interaction with Electronic Systems, SAE-AE4L Committee Report, October 1987.

PRESTO Digital Computer Code User's Guide - Volumes I to VI, DNA Report 3898F, October 1980.

Pryzby, J. E. and J. A. Plumer, Lightning Protection Guidelines and Test Data for Adhesively Bonded Aircraft Structures, NASA Contractor Report 3762, January 1984.

Riley, L. H., et al, "Lightning Tests of Pershing II," IAGC on Lightning and Static Electricity, June 1984.

Shortess, D. L., W. W. Cooley, and B. G. Melander, "Comparison of Four Lightning Simulation Tests on a Composite Test Bed Aircraft," IAGC on Lightning and Static Electricity, April 1988.

Simpson, M. M. and M. J. Katzer, "In-flight Aircraft Lightning Surface Current Model," IAGC on Lightning and Static Electricity, April 1988.

Sommer, D. L., Protection of Electrical Systems from Electromagnetic Hazards - Design Guide, Boeing Military Airplane Co., AFWAL-TR-81-2118, September 1981.

User's Manual for AC-20-53 - Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning (Draft), September 1987.

Walen, D. B., "Lightning Tests on an All-Composite Helicopter," IAGC on Lightning and Static Electricity, April 1988.

Walko, L. C., A Test Technique for Measuring Lightning-Induced Voltages on Aircraft Electrical Circuits, NASA Report CR-2348, February 1974.

## GLOSSARY

ACTION INTEGRAL. The action integral is a critical factor in the production of damage. It relates to the energy deposited or absorbed in a system. This energy cannot be defined without knowing the resistance of the system. The instantaneous power dissipated in a resistor is $I^2P$. and is expressed in watts. For the total energy expended, the power must be integrated over time to get the total joules, watt-seconds. By specifying the integral of $i(t)^2$ over the time interval involved, a useful quantity is defined for application to any resistance value. In the case of lightning, this quantity is defined as the action integral and is specified as $i(t)^2dt$ over the time the current flows.

ACTUAL TRANSIENT LEVEL. The actual transient level is the level of transients which actually appear at the system interfaces as a result of the external environment. This level may be less than or equal to the transient control level but should not be greater.

AIRCRAFT LIGHTNING INTERACTION. An encounter with lightning that produces sufficient current within or voltages along an aircraft skin or structure to pose a threat to the aircraft electrical/electronic systems, as a result of a direct lightning attachment.

ATTACHMENT POINT. A point of contact of the lightning flash with the aircraft.

CHARGE TRANSFER. The integral of the current over its entire duration, $i(t)dt$, in coulombs.

COMPONENT DAMAGE. Condition arising when the electrical characteristics of a circuit component are permanently altered beyond its specifications.

CORONA. A luminous discharge that occurs as a result of an electrical potential difference between the aircraft and the surrounding atmosphere.

CRITICAL. Functions whose failure would contribute to or cause a failure condition which would prevent the continued safe flight and landing of the aircraft.

DESIGN MARGIN. The difference between the equipment transient design levels and the transient control level.

DIRECT EFFECTS. Any physical damage to the aircraft or onboard systems due to the direct attachment of the lightning channel. This includes tearing, bending, burning, vaporization, or blasting of aircraft surfaces or structures, and damage to electrical/electronic systems.

EQUIPMENT TRANSIENT DESIGN LEVEL. The level of transients which the equipment is qualified to withstand.

EQUIPMENT TRANSIENT SUSCEPTIBILITY LEVEL. The transient level which will result in damage or upset to the system components. This level will be greater than the equipment transient design level.

EXTERNAL ENVIRONMENT. Characterization of the natural lightning environment with idealized waveforms for engineering purposes.

INDUCED VOLTAGES. A voltage produced around a closed path or circuit by changing magnetic or electric fields or structural IR voltages.

INDIRECT EFFECTS. Voltage and/or current transients induced by lightning in aircraft electrical wiring which can produce upset and/or damage to components within electrical/electronic systems.

INTERNAL ENVIRONMENT. The fields and structural IR potentials produced by the external environment, along with the voltages and currents induced by them.

LIGHTNING FLASH. The total lightning event in which charge is transferred from one charge center to another. It may occur within a cloud, between clouds, or between a cloud and the ground. It can consist of one or more strokes, plus intermediate or continuing currents.

LIGHTING LEADER STROKE. The leader forms an ionized path for charge to be channeled towards the opposite charge center. The stepped leader travels in a series of short, luminous steps prior to the first return stroke. The dart leader reionizes the return stroke path in one luminous step prior to each subsequent return stroke in the lightning strike.

LIGHTNING STRIKE. Any attachment of the lightning flash to the aircraft.

LIGHTNING STRIKE ZONES. Locations on the aircraft where the lightning flash will attach or where substantial amounts of electrical current may be conducted between attachment points. The location of these zones on any aircraft is dependent on the aircraft's geometry and operational factors and often varies from one aircraft to another.

LIGHTNING RETURN STROKE. A lightning current surge that occurs when the lightning leader makes contact with the ground or an opposite charge center.

MULTIPLE BURST. A randomly spaced series of bursts of short duration, low amplitude current pulses, with each pulse characterized by rapidly changing currents. These bursts may result from lightning leader progression or branching and may be accompanied by or superimposed on stroke or continuing currents. The multiple bursts appear to be most intense at the time of initial leader attachment to the aircraft.

MULTIPLE STRIKE. Two or more lightning strikes during a single flight.

MULTIPLE STROKE. Two or more return strokes occurring during a single lightning flash.

PEAK RATE OF RISE. The maximum instantaneous slope of the waveform as it rises to its maximum value. Mathematically, the peak rate of rise of a function, i(t), may be expressed as the maximum of d[i(t)]/dt.

RETURN STROKE. See lightning return stroke.

STRUCTURAL IR VOLTAGE. The portion of the induced voltage resulting from the product of the distributed lightning current, I, flowing through the resistance, R, of the aircraft skin or structure.

SWEPT STROKE. A series of successive attachments due to sweeping of the flash across the surface of the airplane by the motion of the airplane.

SYSTEM FUNCTIONAL UPSET. Impairment of system operation, whether permanent or momentary (e.g., a change of digital or analog state) which may or may not require manual reset.

TRANSIENT CONTROL LEVEL. The maximum allowable level of transients appearing at the systems interfaces as a result of the defined external environment.

TRIBOELECTRIC CHARGING. Static electricity produced on a structure from the effects of friction.

UPSET. See system functional upset.

## LIST OF ACRONYMS

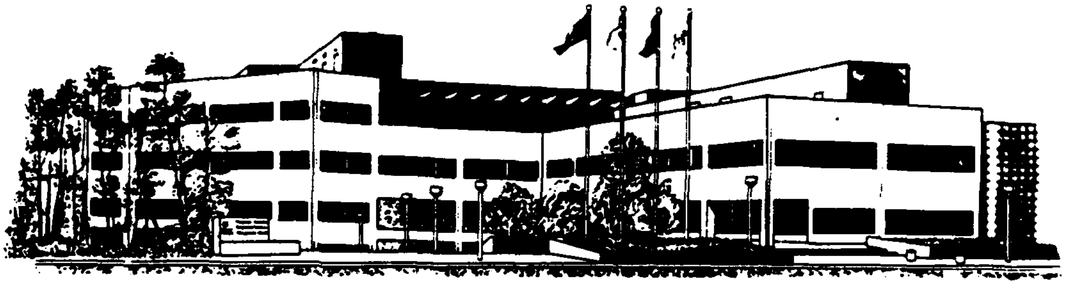
| | |
|---|---|
| ACAP | Advanced Composite Airframe Program |
| ACES | Applied Computational Electromagnetics Society |
| AEHP | Atmospheric Electricity Hazards Protection |
| AE4L | SAE Subcommittee (Lightning) |
| AFFDL | Air Force Flight Dynamics Laboratory |
| AFWAL | Air Force Wright Aeronautical Laboratories |
| ALCM | Air Launched Cruise Missile |
| B-dot | Derivative of the magnetic field with respect to time |
| CW | Continuous Wave |
| DNA | Defense Nuclear Agency |
| DOE | Department of Energy |
| E-dot | Derivative of the electric field with respect to time |
| EM | Electromagnetic |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| EMP | Electromagnetic Pulse |
| ETDL | Equipment Transient Design Level |
| FAA | Federal Aviation Administration |
| G/E | Graphite Epoxy |
| GEMACS | General Electromagnetic Model for the Analysis of Complex Systems |
| HF | High Frequency |
| I | Current |
| I-dot | Derivative of the current with respect to time |
| kA | Kiloampere |
| LF | Low Frequency |
| LPN | Lumped Parameter Network |
| LRU | Line Replaceable Unit |
| LTRI | Lightning and Transients Research Institute |
| NASA | National Aeronautics and Space Administration |
| NASC | Naval Air Systems Command |
| NEC | Numerical Electromagnetics Code |
| NSWC | Naval Surface Weapons Center |
| R | Resistance |
| RAE | Royal Aircraft Establishment |
| RF | Radio Frequency |
| RL | Resistance/Inductance |
| RLC | Resistance/Inductance/Capacitance |
| RLCM | Resistance/Inductance/Capacitance/Mutual |
| SAE | Society of Automotive Engineers |
| TCAP | Threshold Circuit Analysis Program |
| TCL | Transient Control Level |
| TTL | Transistor-Transistor Logic |
| TWTD | Thin Wire Time Domain |
| UHF | Ultra-high Frequency |
| UK | United Kingdom |
| VHF | Very High Frequency |

Department of Transportation
**Federal Aviation Administration**

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II DIGITAL SYSTEMS VALIDATION

## CHAPTER 14
## HIGH ENERGY RADIO FREQUENCY FIELDS (IMPACT ON DIGITAL SYSTEMS)



PREPARED BY:

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

PREPARED FOR:

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF ILLUSTRATIONS (Continued)

## LIST OF TABLES

# 1. INTRODUCTION

## 1.1. Background

The introduction of a new generation of aircraft (fixed wing, rotary wing, and powered lift) advanced technologies, composite structures, and sophisticated high-integrity, integrated, software-based, digital flight control and avionic systems has confronted the aviation community with numerous flight safety issues and concerns. These new aircraft are making use of fly-by-wire flight control systems in which direct mechanical or hydraulic linkages are being replaced by solid-state digital electronic systems controlling engines, fuel systems, and electrohydraulic/electromechanical actuators. Previously, flight control and avionic systems utilized analog technology which was not responsive to transient disturbances unless they exceeded the analog device damage level. Unlike their analog predecessors, digital electronics are very susceptible to transient effects, as well as to discrete-frequency radiation. Digital device performance can be adversely affected (upset) before the device damage level is reached.

A number of European military aircraft fatal accidents have been attributed to High Energy Radio Frequency (HERF). A digital fly-by-wire military Toronado aircraft and crew were lost during a tactical training strafing attack in Germany. The loss was attributed to HERF when the aircraft flew through a high intensity Radio Frequency (RF) field. The civil/military aviation industry has very limited experience or data directed to accidents caused by electromagnetic transients and/or radiation. The present criteria, specifications, and procedures are being reevaluated. The HERF fields apparently upset the digital flight control system of the Toronado which was qualified to a very low Electromagnetic Environment (EME) standard.

While composite materials may offer significant advantages in strength, weight, and cost, they provide less electromagnetic shielding than aluminum. The use of solid-state digital technology in flight critical systems creates major challenges to prevent transient susceptibility and upset in both civil and military aircraft. Therefore, the Civil Aviation Authority (CAA), United Kingdom (U.K.) and the Federal Aviation Administration (FAA), United States (U.S.) voiced concern relative to emerging technology aircraft and systems.

The present criteria, specifications, and procedures appear to be inadequate for industry and the certification authorities for three reasons: (1) the changes in aircraft construction from aluminum to composites, (2) the increased criticality of software-based digital flight control and avionic systems, and (3) the increased levels of RF energy over a wide range of frequencies. The CAA and FAA therefore decided that the impact of each of these areas on the total aircraft RF susceptibility hardening and protection should be assessed.

## 1.2. Objectives and Scope

Currently, the U.S. civil aircraft manufacturers use the electromagnetic susceptibility guidelines as referenced in the Radio Technical Commission for Aeronautics (RTCA) document RTCA/DO-160B, section 20. Category Z equipment qualified to this standard is demonstrated to perform satisfactorily when subjected to a 1 Volt per meter (V/m) electric field intensity for frequencies between 35 MHz and 1215 MHz (a 2 V/m standard is imposed for the Very High Frequency (VHF) communication band from 118 to 136 MHz). A similar standard is used for frequencies between 15 kHz and 35 MHz but is specified in different terms, with a slightly higher standard for the High Frequency (HF) band between 2 and 30 MHz. The European Toronado aircraft was designed and protected according to a similar specification.

The U.S. military qualification standards for RF susceptibility are contained in MIL-STD-461B, section 19. This standard calls for an electric field strength 5 to 20 times greater than that called for in the RTCA document. It also extends the frequency range to at least 10,000 MHz and possibly to 40,000 MHz. This document implies that an electric field of at least 200 V/m may be encountered at specific frequencies which are specified by the procuring command. Testing methods are described in MIL-STD-462. The U.S. Navy, in qualifying aircraft for a carrier flight deck, has defined high electric field intensities greatly exceeding the values of MIL-STD-461B. A number of current military aircraft have encountered Electromagnetic Compatibility (EMC) problems, including the UH-60 helicopters. EME considerations for equipment design and procurement are described in MIL-STD-235-1A.

There have been no recognizable problems reported on civil transport airplanes to date. However, fly-by-wire technology is in use today on some Boeing Model 757-200 and 747-400 airplanes, on the Airbus Industrie A-320, Pratt and Whitney 4000° engines, and other U.S. civil aircraft (fixed and rotary wing). In addition, civil and military transmitter systems are continually being upgraded to operate at higher frequencies and to produce higher effective electric field intensities. The Spectrum Engineering Division of the FAA Technical Center and the Aircraft Engineering Division in the Office of Airworthiness initiated a research effort with the Department of Defense (DOD), Electromagnetic Compatibility Analysis Center (ECAC), Annapolis, Maryland, to survey the Contiguous United States (CONUS) and its possessions for civil and military ground, airborne, and shipborne HERF sources. Simultaneously, a solicitation for the CAA and its European counterparts to aggressively conduct a similar survey and analysis was requested. Following the surveys by ECAC, a validation phase (airborne measurements) of selected transmitters and one airport was conducted by Ohio University, Athens, Ohio.

United States research initiatives include:

- Conducting research into worldwide civil and military ground, airborne, and shipborne emitter radiation which may be a threat to emerging aircraft and systems.

- Sharing knowledge of each country's (i.e., United States, United Kingdom, and France) civil and military high powered transmitters.

- Developing the best approach to transfer this information to the airframe and systems manufacturers, RTCA, Society of Automotive Engineers (SAE), European Organization for Civil Aviation Electronics (EUROCAE), International Civil Aviation Organization (ICAO), etc.

- Developing an international susceptibility standard.

- Investigating possible regulatory actions (i.e., Notice of Proposed Rulemaking (NPRM), Advisory Circular (AC), User's Manual, etc.).

- Considering the airworthiness, certification, and operational issues and implications.

In addition to these initiatives, the Flight Safety Research Branch at the FAA Technical Center is participating in an Electromagnetic Radiation (EMR) measurement test being conducted by the U.S. Air Force Special Missions Operational Test and Evaluation Center (SMOTEC), Hurlburt Field, Florida. The primary purpose of this test is to collect EMR data at selected locations to enable safe air transport of munitions. Experience has shown that when an electromagnetic field impinges on a munition, it can fire the electroexplosive devices, destroy transistors, or cause electronic circuits to malfunction. Examples of the multitude of threats considered in this chapter are illustrated in figure 1.2-1.

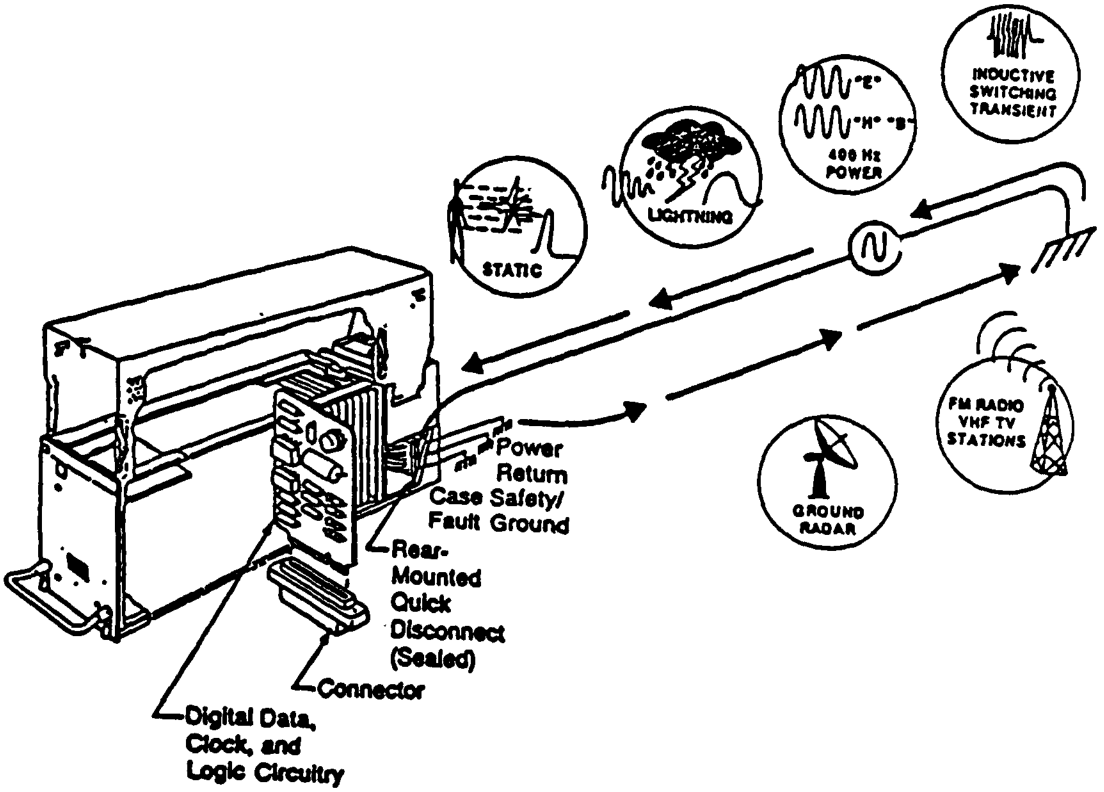

INDUCTIVE SWITCHING TRANSIENT
"E"
"H" "B"
400 Hz POWER
LIGHTNING
STATIC
FM RADIO VHF TV STATIONS
GROUND RADAR
Power
Return
Case Safety/ Fault Ground
Rear-Mounted Quick Disconnect (Sealed)
Connector
Digital Data, Clock, and Logic Circuitry

FIGURE 1.2-1. INDUCED RADIO FREQUENCY THREAT

## 2. ELECTROMAGNETIC ENVIRONMENT SURVEY AND ANALYSIS - UNITED STATES

### 2.1. Guidelines

In an effort to standardize prediction techniques, the FAA and ECAC documented the techniques used in the form of guidelines (DOD/ECAC, 1987) for predicting maximum EMR levels at aircraft exposed to high-powered emitters. Those guidelines were used in the calculation of maximum peak and average electric field strengths at the aircraft as a result of ground, airborne, and shipborne RF emitters. The guidelines for calculating peak and average field strengths are presented as step-by-step instructions starting with the data on the emitters in the EME and ending with an envelope graph representing maximum field strengths. The methods for calculating field strengths in the worst-case scenario and in the takeoff and landing scenario are defined and discussed. Simplifying assumptions are made and, where appropriate, justifications are shown. The minimum distances used in the U.S. environmental analysis are presented. The results obtained by following these guidelines will be peak and average field strengths, at worst case distances between emitters in the EME and aircraft. The total survey and environment analysis is described as the airport, air-to-air, ground, and shipborne environment.

Scenarios for the survey and analysis guidelines are as follows:

- A worst-case civil or military emitter, and for comparison, a takeoff or landing at specific airports.
- A worst-case considering the maximum EMR levels at an aircraft exposed to any ground, airborne, and shipborne emitter in the United States.
- The EME that would be experienced by an aircraft on takeoff and landing at six major U.S. airports.
- Integration and comparison of the worst-case emitters from the United Kingdom, France, and other countries as their information becomes available.
- Integration and comparison of the American, British, and French airport data.

### 2.2. Results

The results are presented in peak and average field strengths for the aircraft emitter sources surrounding airport, air-to-air, ground, and shipboard areas. The survey would review the emitters from 10 kHz to 40 GHz, identify worst-case conditions, and plot survey and study results in RF envelope histograms. To make the data manageable and unclassified, the granularity of the curve has been smoothed.

The following assumptions were made to simplify the task and the histograms:

- Specification of minimum distances.
- Continuous illumination.
- Mainbeam gain.
- Modulation independence.
- Constructive ground reflections at HF.
- Noncumulative field strengths.
- Near-field correction.

A typical analysis of a specific emitter considered the specifications of each, as indicated in table 2.2-1.

TABLE 2.2-1. FIXED AIRPORT EMITTER

| HEIGHT - FINDING RADAR | |
|---|---|
| Operating Frequency | 2700 MHz |
| Peak/Average Output Power | 3.5 MW/2.9 kW |
| Antenna Size | 8 ft x 30 ft |
| Antenna Gain | 39 dBi |
| Distance | 500 ft |
| **ELECTRIC - FIELD STRENGTH** | |
| Uncorrected Peak | 6050 V/m |
| Uncorrected Average | 175 V/m |
| Near Field | 700 ft |
| Near Field Correction Factor | 3.5 dB |
| Corrected Peak | 4100 V/m |
| Corrected Average | 120 V/m |

## 2.3. Airport Environment

The airport environment consists of fixed and mobile emitters located on the airport. The airport is defined by a five nautical mile (nmi) radius from the geographic center of the airport. Minimum distance calculations are for airport fixed emitters and mobile emitters. By regulations, the minimum distance between a fixed emitter and the taxiway or runway is 250 feet (ft). Table 2.3-1 identifies some fixed emitters at the airport.

TABLE 2.3-1. FIXED AIRPORT ENVIRONMENT

| |
|---|
| Marker Beacon |
| Localizer |
| VOR |
| Glide Slope |
| Ground Controlled Approach Radar |
| Distance Measuring Equipment |
| TACAN |
| Microwave Landing System |
| Airport Surface Detection System |
| Non-Directional Beacon |
| Airport Surveillance Radar |
| Air Route Surveillance Radar |
| Weather Radar |
| ATCRBS Interrogator |
| VHF and UHF Communications/Telemetry |

For fixed airport emitters above, predicted maximum peak and average field strengths were calculated and plotted as in figures 2.3-1 and 2.3-2.

The mobile emitter environment consists of all emitters that are not in a fixed location within a minimum distance of 50 ft. These include those emitters on ground support vehicles as well as those in aircraft. Aircraft emitters may operate while on the ground and taxiway, and prior to takeoff. Table 2.3-2 outlines those mobile emitters.

For mobile airport emitters above, predicted maximum peak and average field strengths were calculated and plotted as in figures 2.3-3 and 2.3-4.

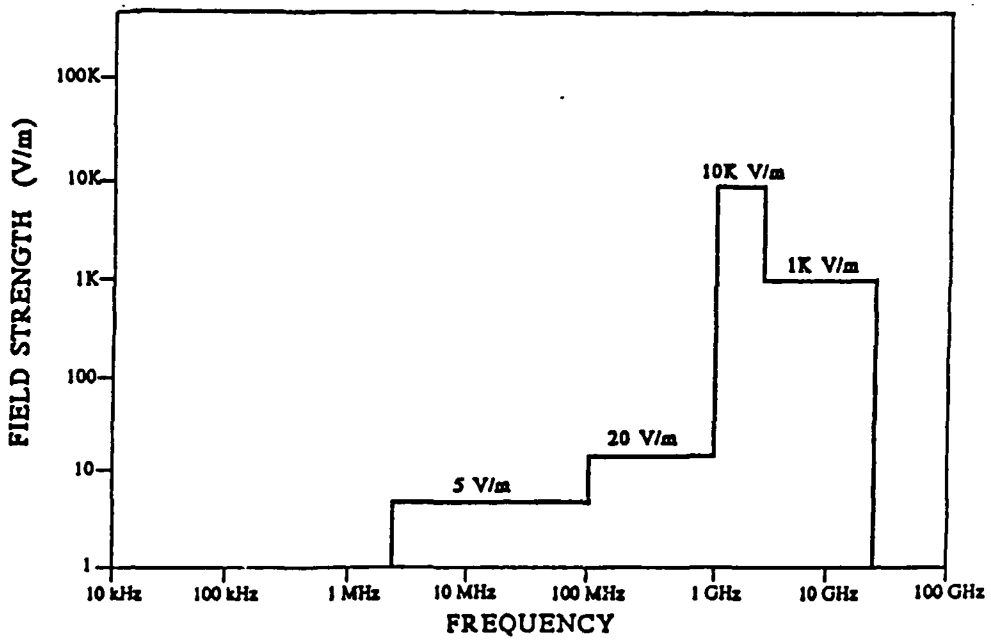


FIGURE 2.3-1. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS FROM CIVILIAN AIRPORT FIXED EMITTERS

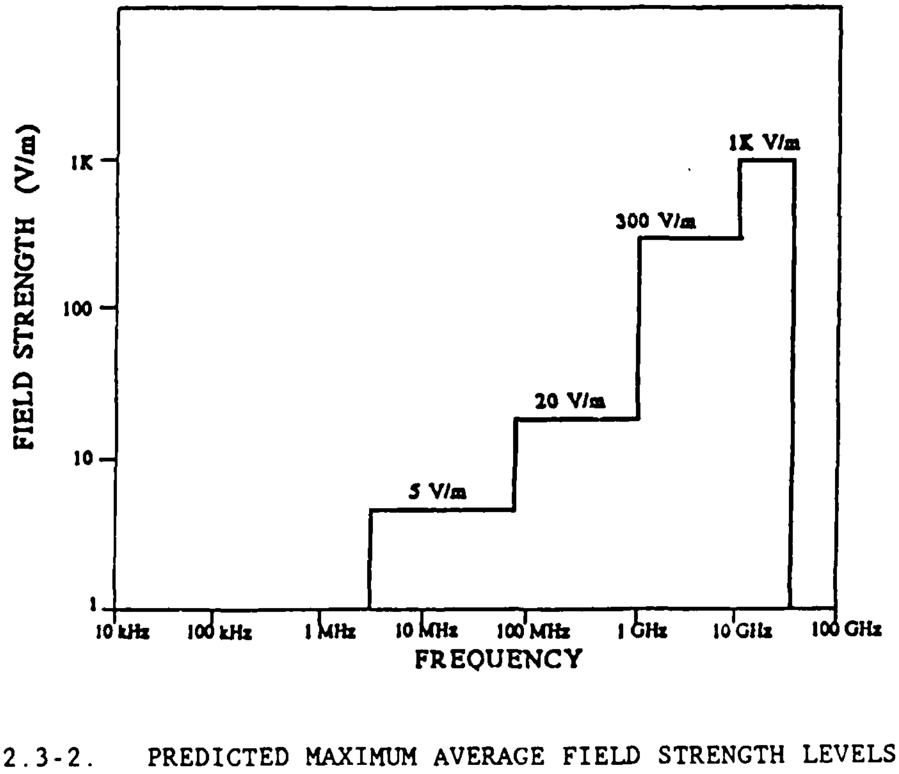


FIGURE 2.3-2. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS FROM CIVILIAN AIRPORT FIXED EMITTERS

TABLE 2.3-2. MOBILE AIRPORT ENVIRONMENT

HF/VHF/UHF Communications
Tacan
Doppler Navigational Radar
Radio Altimeter
Weather Radar
ATCRBS Beacon

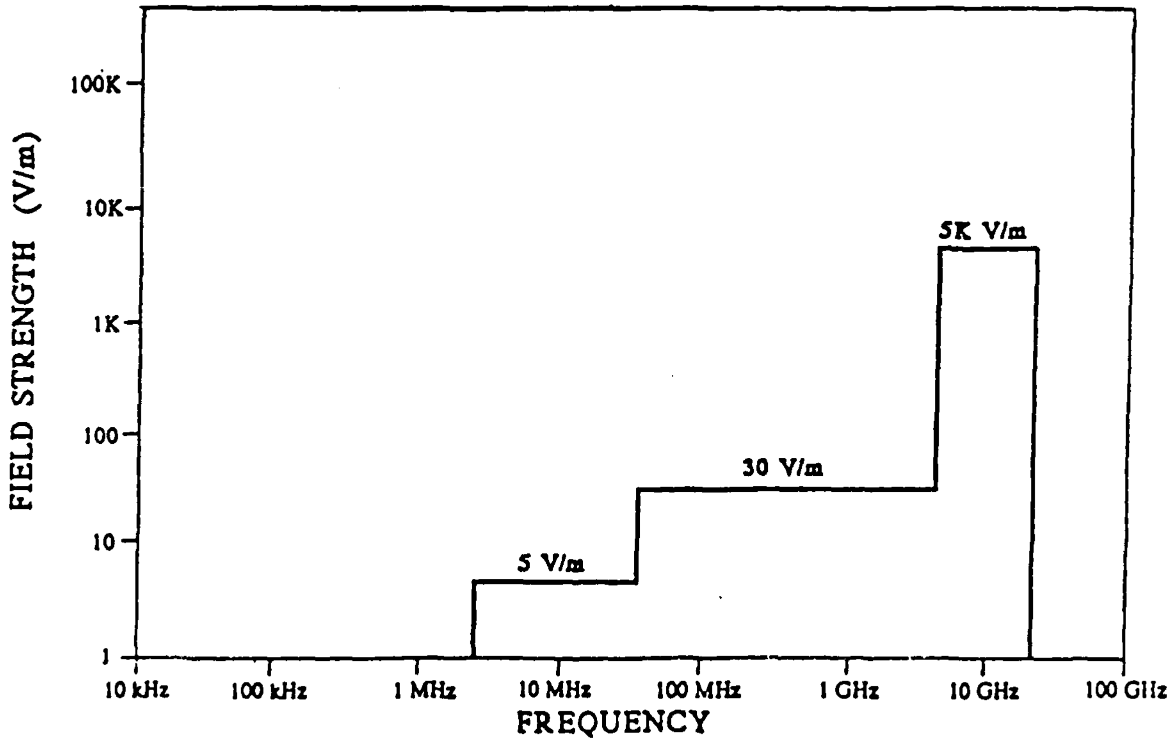


FIGURE 2.3-3. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS FROM CIVILIAN AIRPORT MOBILE EMITTERS

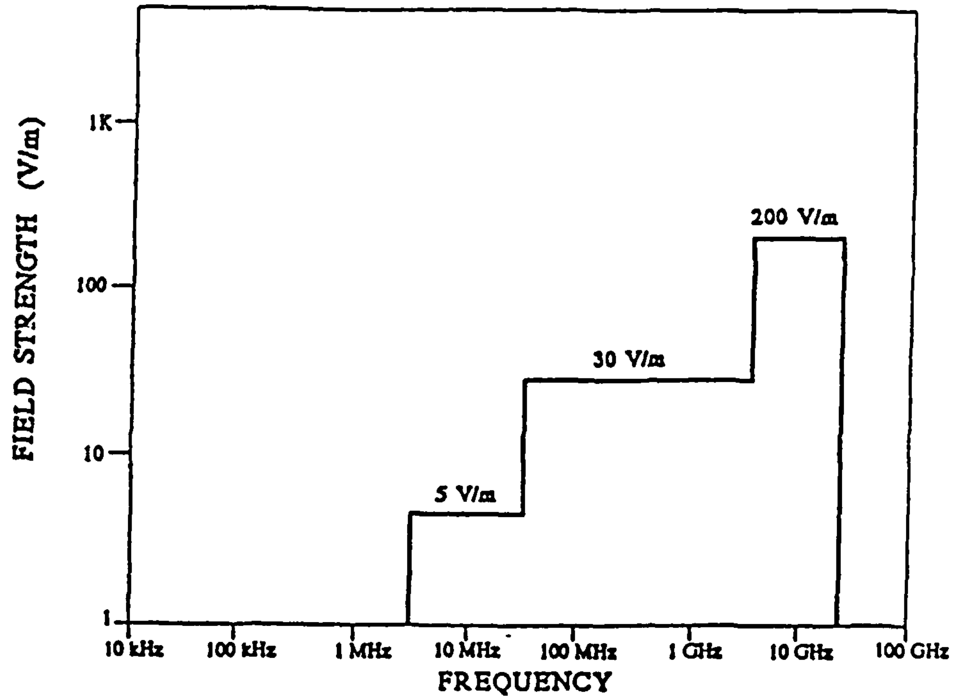


FIGURE 2.3-4. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS FROM CIVILIAN AIRPORT MOBILE EMITTERS

## 2.4. Air-to-Air Environment

In the air-to-air environment, normally, only military aircraft are considered. An interceptor aircraft may approach as close as 50 ft to an unidentified commercial aircraft while trying to establish its identity. Very high powered military Electronic Counter Measures (ECM) systems will be assumed as not operating at this close range. Non-interceptor aircraft, Airborne Warning and Control System (AWACS) or ECM aircraft would not intentionally approach closer than 500 ft but could be operating high-powered emitters. Predicted peak and average field strengths are calculated and plotted for the interceptor and noninterceptor aircraft in figures 2.4-1 through 2.4-4.

## 2.5. Ground Environment

The ground environment is the largest of the four environments since it includes all fixed and ground mobile emitters not located on an airport. These emitters are located at a distance greater than 5 miles from the center of the airport. The ICAO aircraft minimum obstruction clearance is 500 ft above ground level. The 500-ft minimum distance was used for field strength calculations; therefore, this places the aircraft within the near field of the emitting antenna. The ground equipment includes those types in table 2.5-1.

Predicted maximum peak and average field strengths are calculated and plotted for the ground environment equipment in figures 2.5-1 and 2.5-2.

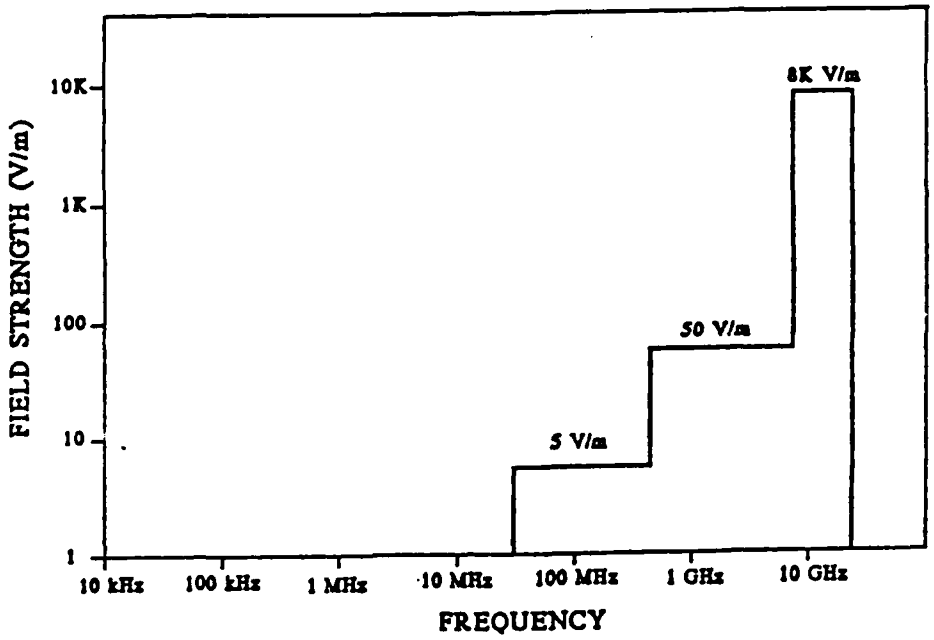


FIGURE 2.4-1. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS FROM INTERCEPTOR AIRCRAFT EMITTERS

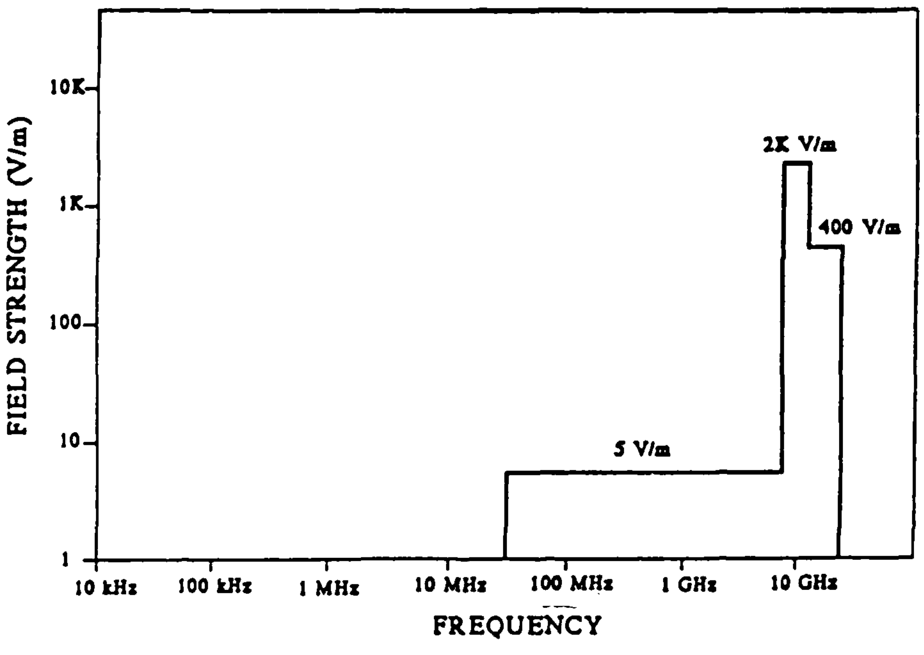


FIGURE 2.4-2. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS FROM INTERCEPTOR AIRCRAFT EMITTERS

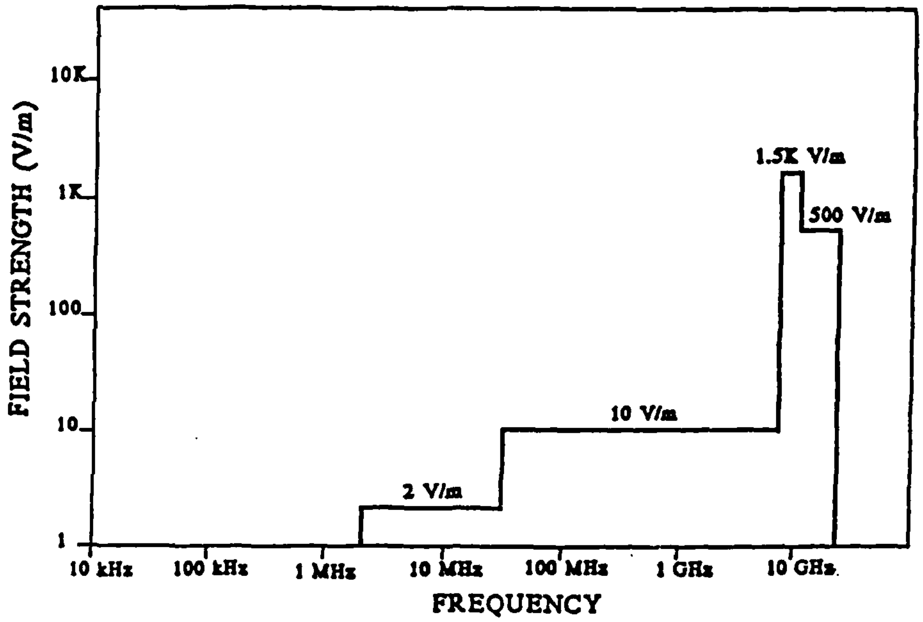


FIGURE 2.4-3. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS FROM MILITARY NON-INTERCEPTOR AIRCRAFT

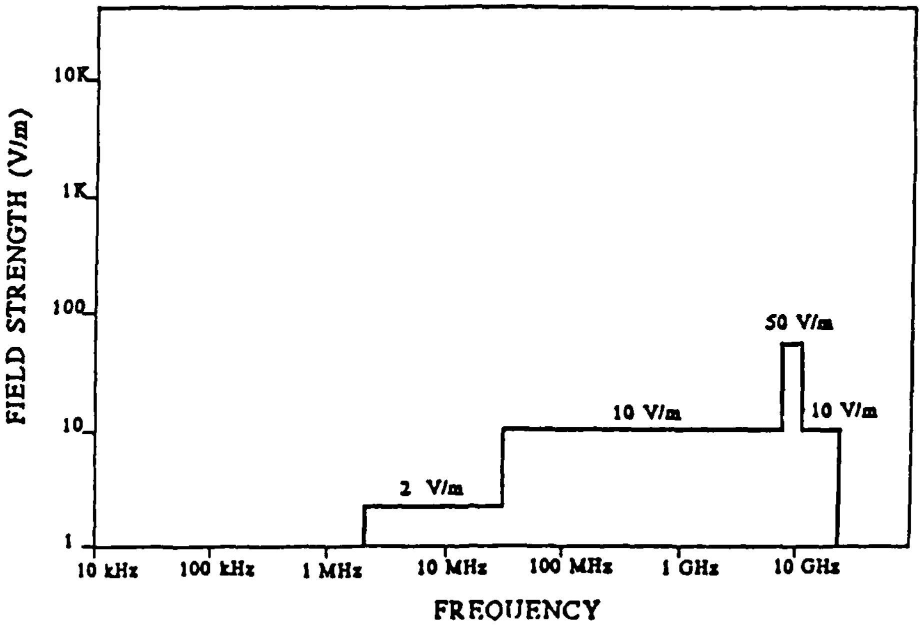


FIGURE 2.4-4. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS FROM MILITARY NON-INTERCEPTOR AIRCRAFT

TABLE 2.5-1. GROUND EQUIPMENT

Radars
Earth Terminals
Sounders
Troposcatter Communications
Commercial AM, FM, and TV Broadcast Transmitter
Test and Training Equipment

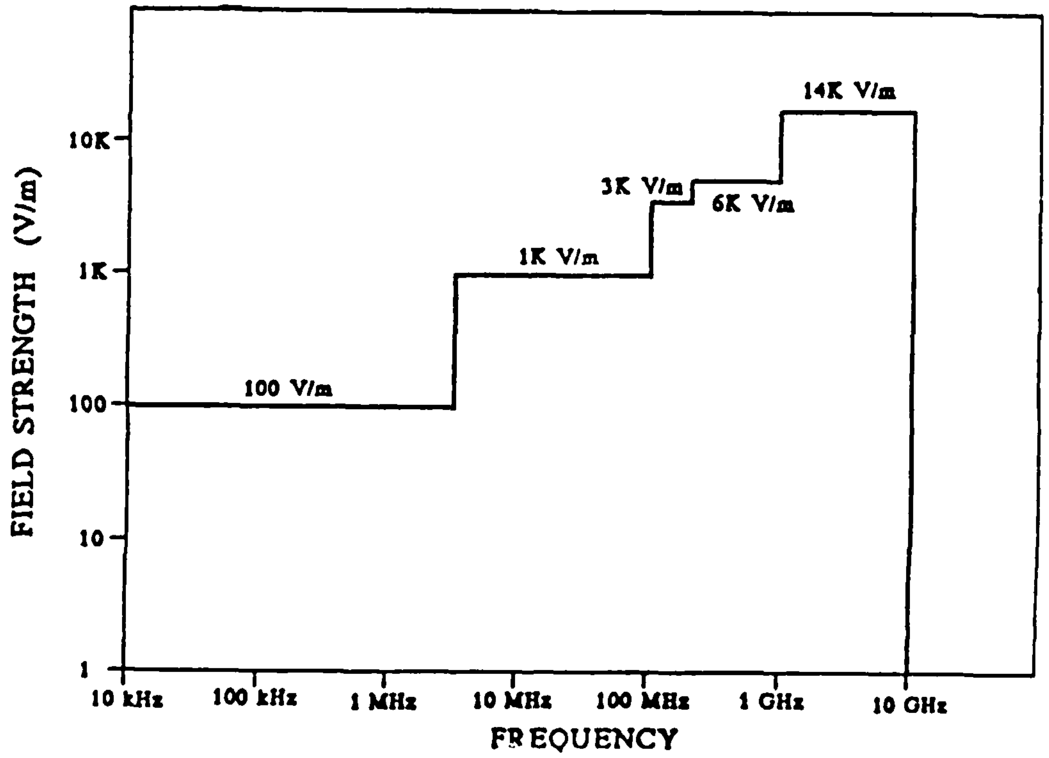


FIGURE 2.5-1. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS FROM GROUND EMITTERS

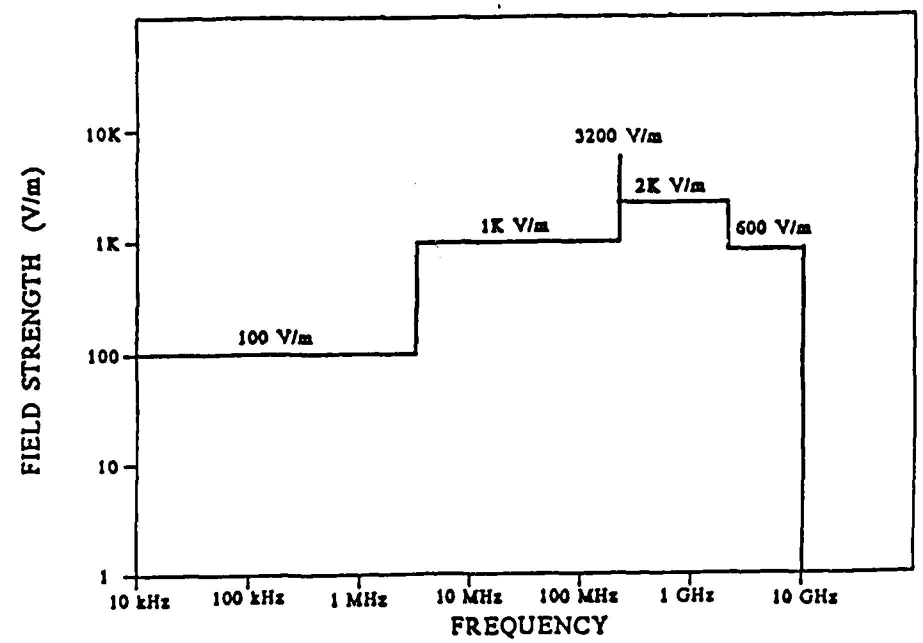


FIGURE 2.5-2. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS FROM GROUND EMITTERS

## 2.6. Shipboard Environment

A number of U.S. and international airports are located near harbors, shipping lanes, etc.; therefore, approach to landing and takeoff paths may cross over commercial and/or military ships, i.e., oil transports, cruise liners, aircraft carriers, and support vessels. Some of these ships, i.e., aircraft carriers, contain very high-powered emitters at high frequencies. A minimum distance of 1000 ft was considered for the field strength calculations. The shipboard equipment includes those types listed in table 2.6-1.

Predicted maximum peak and average field strengths are calculated and plotted for shipboard equipment in figures 2.6-1 and 2.6-2.

TABLE 2.6-1. SHIPBOARD EQUIPMENT

| |
|---|
| Search Radars |
| Track Radars |
| IFF/SIF |
| HF and UHF Communications |

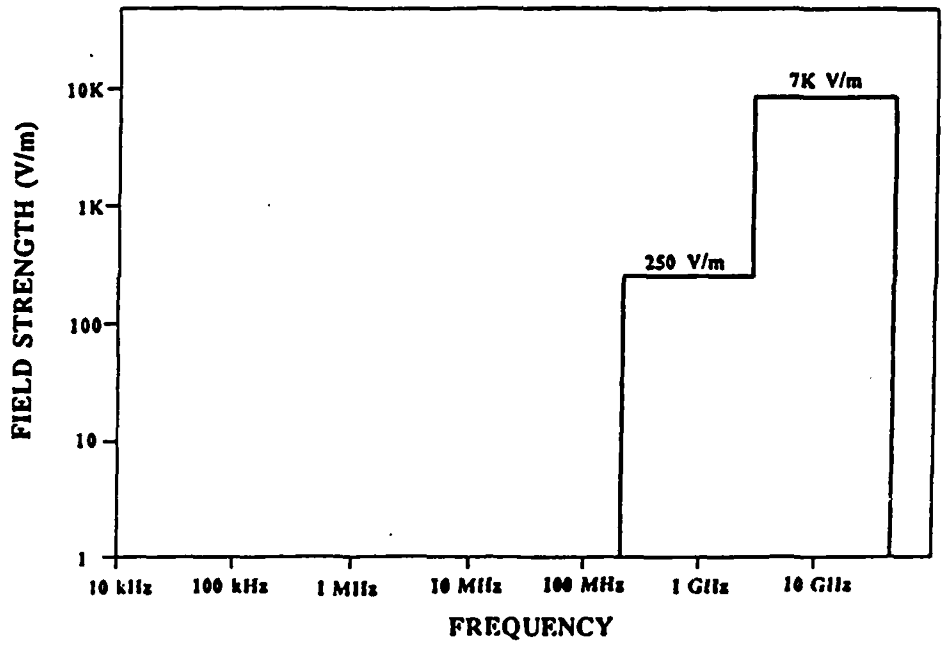


FIGURE 2.6-1. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS FROM SHIPBOARD EMITTERS

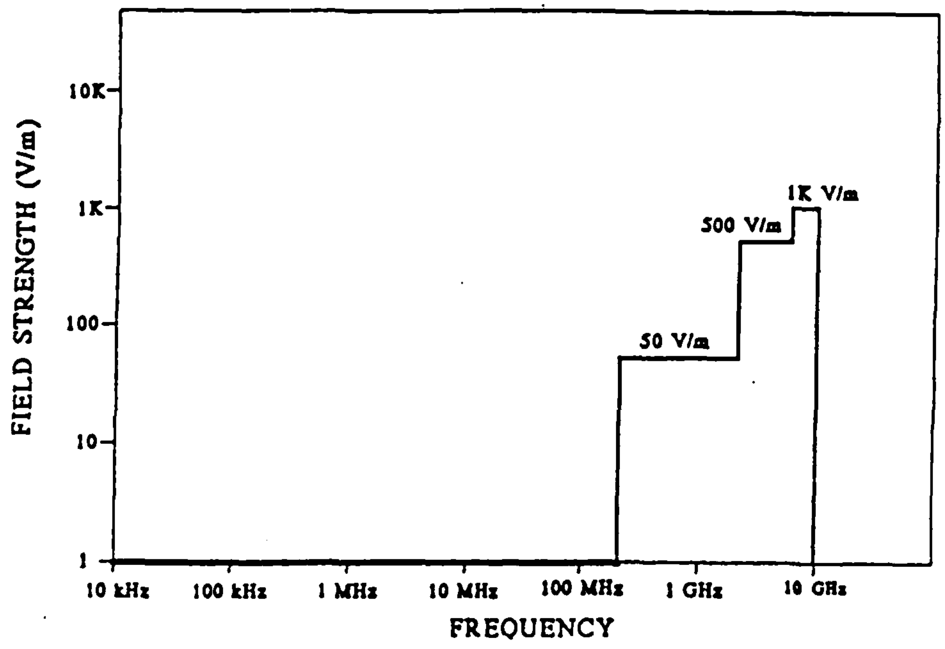


FIGURE 2.6-2. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS FROM SHIPBOARD EMITTERS

## 2.7. Composite of United States Emitters

The airport, air-to-air, ground, and shipboard peak and average field strengths were integrated into electric field strengths for the total U.S. environment. The U.S. environment includes both civil and military emitters. Predicted maximum peak and average field strengths are calculated and plotted for composite U.S. emitters in figures 2.7-1 and 2.7-2.

## 2.8. Composite of United States Compared to NATO STANAG 3614AE

Tracking of the total U.S. environment and the North Atlantic Treaty Organization (NATO) STANAG is remarkably close. The U.S. environment is not as granular as the NATO environments. In the early FAA and ECAC analysis, the charts were more granular, and the decision was made to present the data in a fashion as not to give enough information that would compromise the classified military emitters. Figures 2.7-1 and 2.7-2 are more granular than figure 2.8-1.

## 2.9. Takeoff and Landing Scenario

For minimum distance determination on and around airports, the worst-case condition is the engine out situation for a two-engine aircraft. The aircraft performance and FAA criteria dictates that the aircraft climb to and maintain a minimum altitude prior to initiating a go-around. Figure 2.9-1 shows the FAA criteria and the minimum altitudes that the aircraft must maintain.

The minimum distance between an aircraft and an emitter is dependent on the location of the emitter and the altitude of the aircraft. Where appropriate, the height of the emitting antenna above ground should be deducted from the aircraft minimum altitude to obtain the minimum distance from that specific emitter.

Based on the above criteria, minimum distances for field strength calculations can be estimated as follows:

- As expressed in the airport analysis above, a minimum distance of 250 ft is described near airport runways or taxiways.

- In an engine-out situation, the aircraft must be at an altitude of 35 ft at threshold (end of runway), climbing at a minimum gradient of 2.4 percent.

  This places the aircraft at an altitude of 300 ft at a distance of 1.84 nmi from the end of the runway.

- The aircraft will be at an altitude of 300 ft to a distance of 4.5 nmi from the end of the runway.

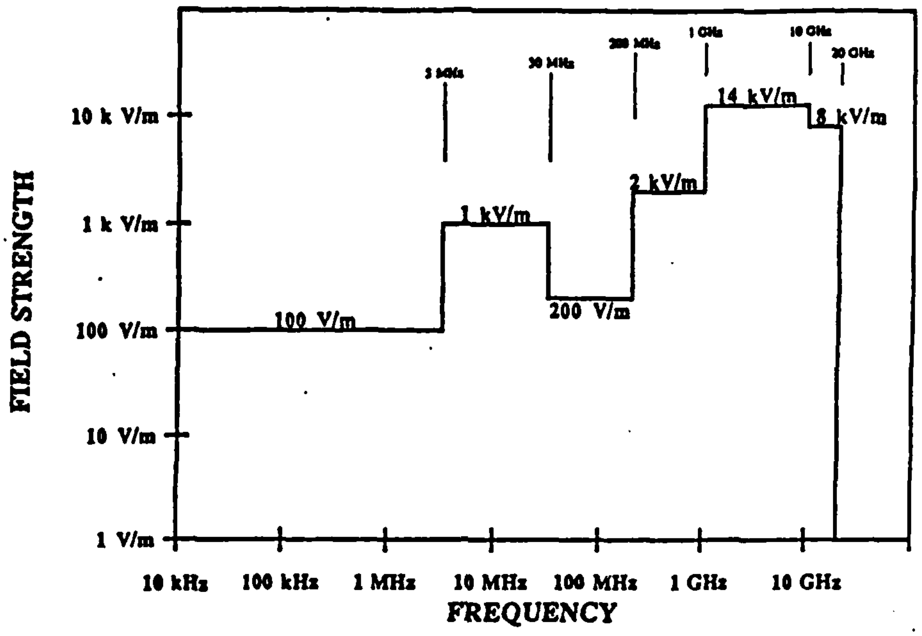


FIGURE 2.7-1. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS COMPOSITE OF UNITED STATES EMITTERS

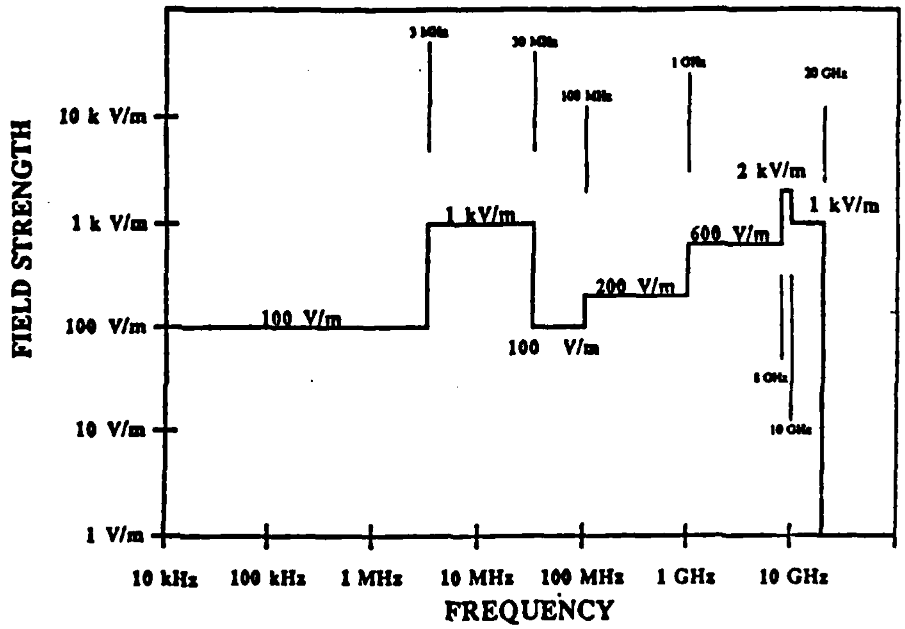


FIGURE 2.7-2. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS COMPOSITE OF UNITED STATES EMITTERS

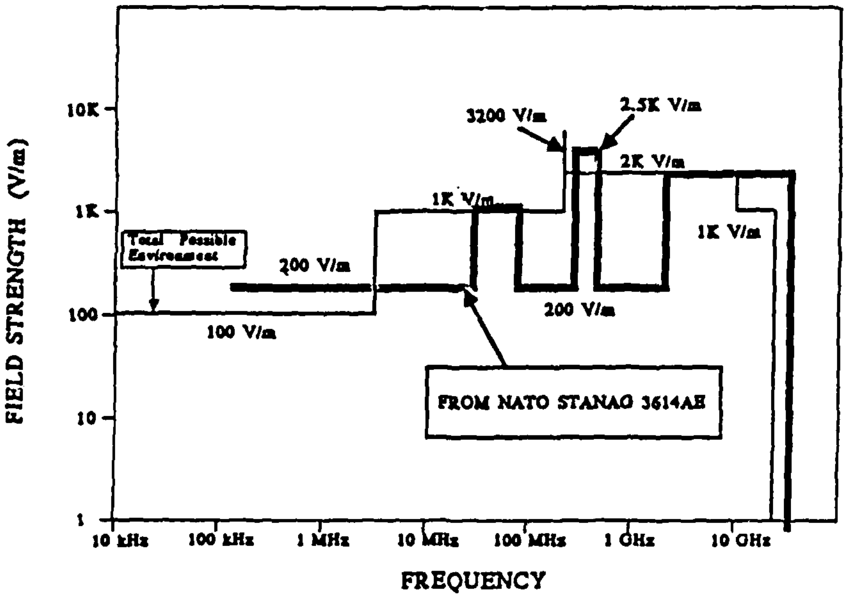


FIGURE 2.8-1. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS UNITED STATES COMPOSITE VS NATO STANAG 3614AE

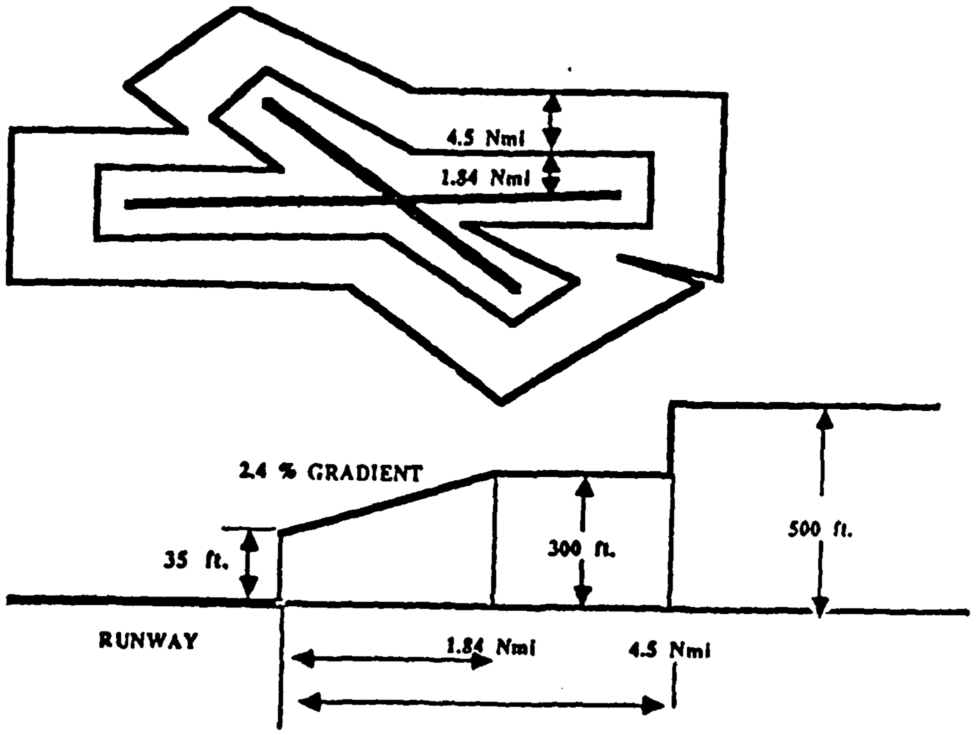


FIGURE 2.9-1. CRITERIA FOR SUSCEPTIBILITY THRESHOLD

- At 4.5 nmi, the minimum altitude is specified as 500 ft.

Note: In the shipboard environment, the minimum distance was considered to be 1000 ft, but the airport takeoff and landing scenario should be considered for those airports near the shipping lanes, which would reduce the minimum distance from 1000 ft to 300 ft. Recalculation of the peak and average field strengths in the shipboard environment is in progress.

The six airports that were examined in the United States are Baltimore, Honolulu, New York (Kennedy), Los Angeles, Seattle, and Denver (Stapleton). They were selected as being representative and typical of U.S. airports with certain unique local environments, industry, seaports, etc.

It is possible that the field strength levels may be higher at other airports than for the six airports selected, but there is a confidence level for those data being representative.

Peak and average field strengths were calculated for each airport, resulting in 12 graphs. Two composite graphs were developed from the 12 individual graphs. They are compared and overlaid in figures 2.9-2 and 2.9-3.

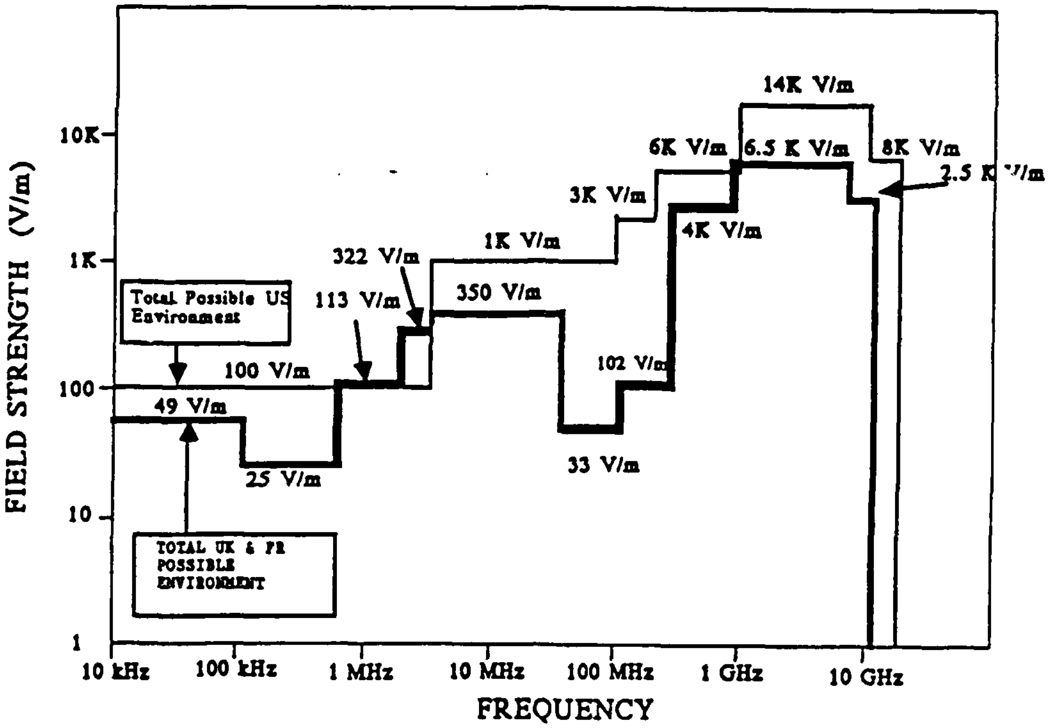


FIGURE 2.9-2. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS COMPARISON UNITED STATES COMPOSITE WITH SIX AIRPORT COMPOSITE

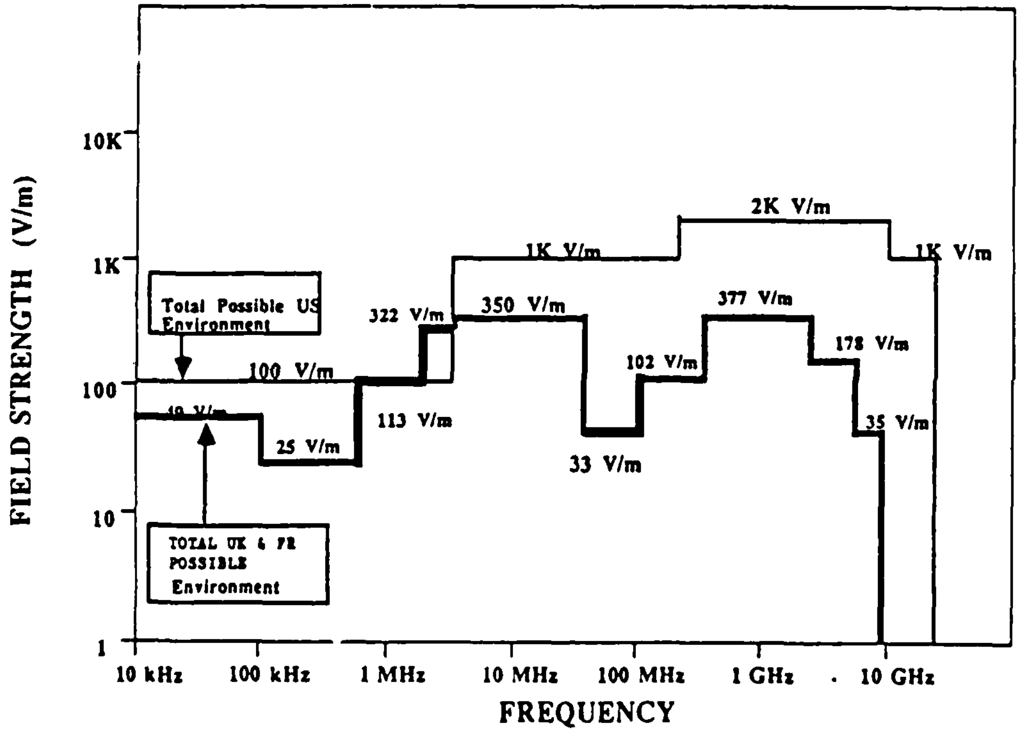


FIGURE 2.9-3. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS COMPARISON UNITED STATES COMPOSITE WITH SIX AIRPORT COMPOSITE

## 3. EME SURVEY AND ANALYSIS - WORLDWIDE

### 3.1. Guidelines

The CAA, U.K., initiated requests for other European countries to participate in this HERF survey and to study each country's own emitter environments. Initially, only the United Kingdom and France responded and aggressively supported this total effort. Their results are presented herein. In September 1987, 27 countries were invited to support and participate in an International Conference in Washington, D.C. Ten countries attended including the United States, United Kingdom, and France. Canada and Sweden were the only other countries in which preliminary surveys were conducted. Sweden's early results were presented at this conference by the Swedish representative.

In April of 1988, a similar international conference was conducted in Brighton, England. The same 27 countries were invited to participate and present their survey data. Australia and West Germany provided an overview of their preliminary data.

British, French, and Swedish technical teams used the FAA and ECAC format as guidelines for their survey and analysis. France, associated with its survey and analysis, conducted an extensive airborne (rotorcraft) measurement program for selected emitters. The U.S. measurement and validation effort was conducted by the FAA, ECAC, and Ohio University. The summary of these efforts will be described later in the validation study currently in progress.

### 3.2. Results

Results are presented in a comparison of the American worst-case total environment to the composite of the British and French survey data. Figures 3.2-1 and 3.2-2 show the predicted maximum peak and average field strength levels for this comparison.

Figures 3.2-3 and 3.2-4 show composite worst-case environment for all three countries.

Figures 3.2-5 and 3.2-6 show U.S. airports (Baltimore, Honolulu, Kennedy, Los Angeles, Seattle, Denver (Stapleton)) integrated with the British airports (Heathrow, Manchester, Glasgow) and the French airports (Orly, Toulouse, Lyon, Nice).

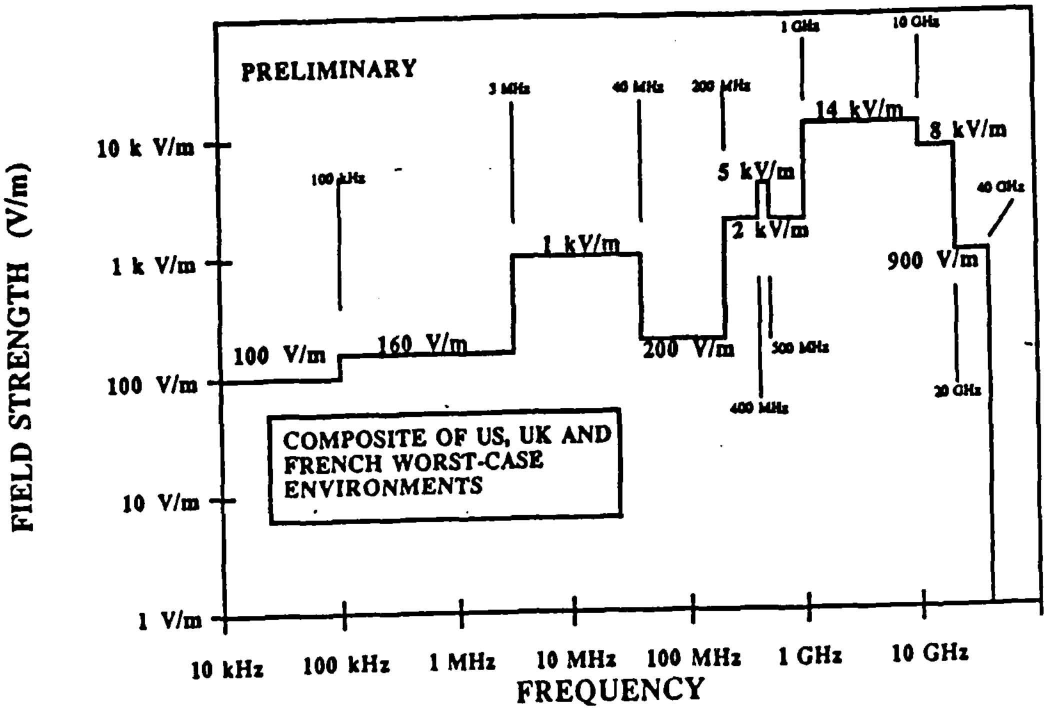


FIGURE 3.2-1. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS COMPARISON OF UNITED STATES COMPOSITE WITH UNITED KINGDOM AND FRANCE COMPOSITE

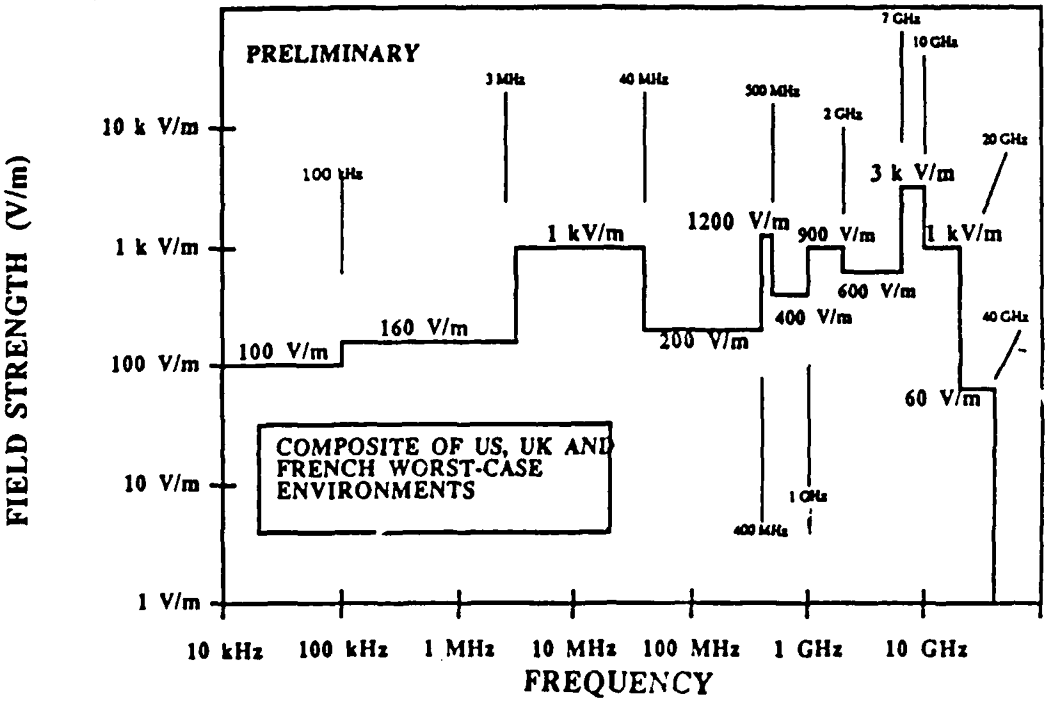


FIGURE 3.2-2. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS COMPARISON OF UNITED STATES COMPOSITE WITH UNITED KINGDOM AND FRANCE COMPOSITE

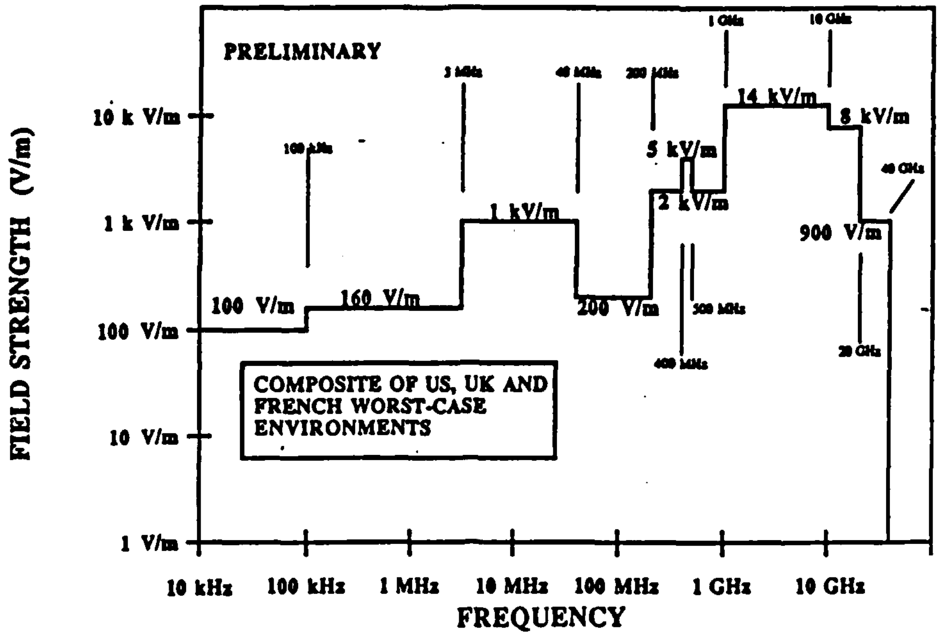


FIGURE 3.2-3. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS WORLDWIDE WORST-CASE ENVIRONMENT

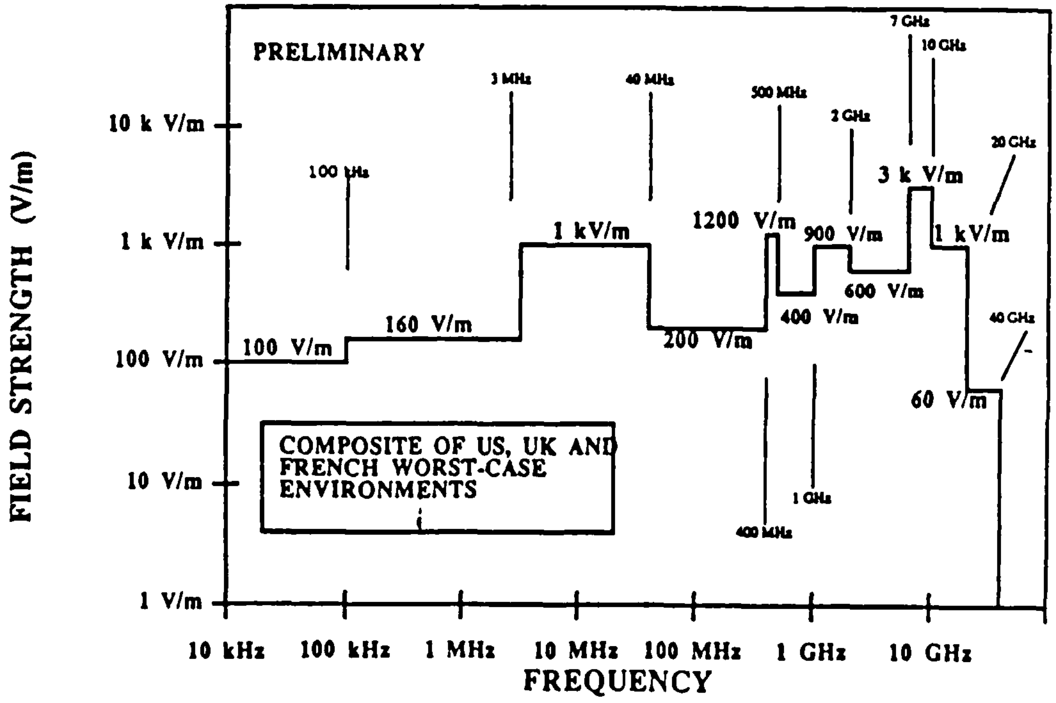


FIGURE 3.2-4. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS WORLDWIDE WORST-CASE ENVIRONMENT

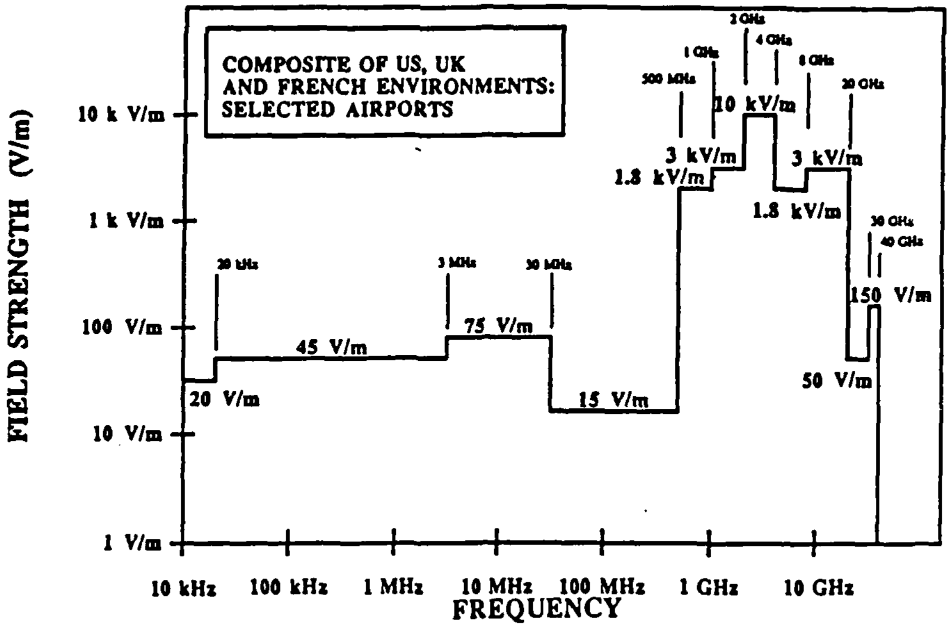


FIGURE 3.2-5. PREDICTED MAXIMUM PEAK FIELD STRENGTH LEVELS COMPOSITE OF INTERNATIONAL ENVIRONMENTS

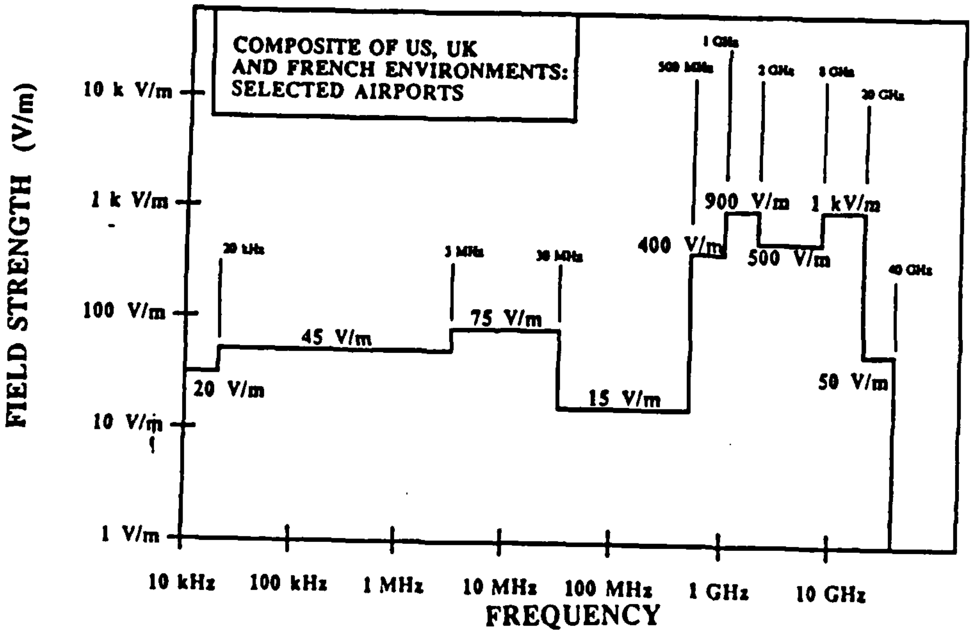


FIGURE 3.2-6. PREDICTED MAXIMUM AVERAGE FIELD STRENGTH LEVELS COMPOSITE OF INTERNATIONAL ENVIRONMENTS

## 4. COMMENTS

Based on the initial survey and analysis of our current environment, HERF fields are indeed a threat to state-of-the-art civil and military aircraft being placed into service throughout the world. Modern aircraft with composite construction, VLSI computers, and electronic devices for flight-critical functions have greatly magnified the threat of EMEs to safe flight operations.

The FAA, in concert with the DOD, U.K. CAA, French DGAC, and their European counterparts, are aggressively pursuing the research to meet this challenge. Following the survey and analysis, a validation phase of selected emitters will be conducted by Ohio University and ECAC. The guidelines established will promote uniformity of results from other members of the international aviation community so that all results can be combined and used to develop an international susceptibility standard.

RTCA was solicited by the FAA to establish a HERF subcommittee to update RTCA DO-160B, Section 20 to address the FAA EME as developed. A HERF Working Group was established under the RTCA Special Committee (SC-135) to review the equipment radiation susceptibility levels currently in DO-160B (which are inadequate for the FAA HERF·environment) and then establish an industry-wide aircraft requirement for conducted and radiated susceptibility.

The FAA solicited the SAE-AE4 Committee for the development of procedures and guidance material, relative to HERF fields, which could be used during the aircraft certification process. Based on this request, SAE-AE4R, Aircraft Radiated Environment Subcommittee, was formed. The goal of the subcommittee was to draft an AC and attendant user's manual for guidance and information on HERF use in commercial aircraft.

SAE-AE4R subcommittee established three subcommittees: a Data Accuracy Subcommittee that will look at the exterior electromagnetic RF environment, a Design Approach Subcommittee that will develop design guidance for airframe manufacturers for the defined EME, and a Test and Analysis Methods subcommittee that will focus on validation techniques.

# APPENDIX A

# GUIDELINES FOR DEVELOPING MAXIMUM PEAK AND AVERAGE FIELD STRENGTH ENVELOPE GRAPHS FOR AIRCRAFT

BY ALEXANDER GROSS
OF THE
DOD ELECTROMAGNETIC COMPATIBILITY ANALYSIS CENTER
ON BEHALF OF
THE DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

SEPTEMBER 1987

:

# APPENDIX A - GUIDELINES FOR DEVELOPING MAXIMUM PEAK AND AVERAGE FIELD STRENGTH ENVELOPE GRAPHS FOR AIRCRAFT

## BACKGROUND

The U.S. Federal Aviation Administration (FAA) is concerned with the safety and integrity of new technology transport-category airplanes with fully flight-critical and flight-essential systems. One of their concerns is the protection of these aircraft from electromagnetic radiation (EMR) produced by external high-energy ground and airborne radio-frequency (RF) emitters. The FAA is in the process of developing proposed requirements and standards to address this concern.

As part of this effort, the Electromagnetic Compatibility Analysis Center (ECAC) was requested to predict the maximum EMR levels at aircraft in the United States for two specified scenarios: a worst-case total U.S. scenario and, for comparison, a take-off and landing scenario at specific airports. The worst-case scenario considered the maximum EMR levels at an aircraft exposed to any emitter in the U.S. The second scenario considered the EMR that would be experienced by an aircraft on take-off and landing at six major U.S. airports.

Those results of this study will be used by the FAA in the development of U.S. requirements and standards relating to the effects of transmitted RF energy on flight-critical control and avionics systems aboard modern aircraft. Since aircraft are required to fly throughout the world, an international RF susceptibility standard is also desired. It is suggested that maximum EMR level predictions should be made by other members of the international aviation community to support an international standard. In an effort to standardize the prediction techniques, ECAC has been requested by the FAA to document the techniques that were used by ECAC in the form of guidelines for predicting maximum EMR levels at aircraft exposed to high-powered emitters.

## OBJECTIVE

The objective of this paper is to present those guidelines that were used by ECAC in the calculation of maximum peak and average electric field strengths at transport-category aircraft with fully electronic flight-critical and flight-essential systems as a result of ground and airborne RF emitters. These guidelines are presented to promote uniformity of results from other countries so that all inputs can be combined.

## APPROACH

The guidelines for calculating peak and average field strengths are presented as step-by-step instructions starting with the data on the emitters in the electromagnetic environment (EME) and ending with an envelope graph representing maximum field strengths. The methods for calculating field strengths in the worst-case in the worst-case scenario and in the take-off and landing scenario are defined and discussed. Equations used to estimate missing technical parameters, to calculate the near field of an antenna, and to calculate the field strengths are provided. Simplifying assumptions are made and, where appropriate, justifications are shown. The minimum distances used in the U.S. environmental analysis are presented. The results obtained by following these guidelines will be peak and average field strengths, at worst-case distances between emitters in the EME and aircraft.

## PROCEDURES

### GENERAL ASSUMPTIONS

The calculation of maximum EMR is based on several assumptions. These are:

1. The minimum allowable separation distance between civil aircraft and an RF emitter is used to calculate the maximum electric field strength at the aircraft. The minimum distance is a worst-case distance that is determined by the scenario being considered and by the environment within that scenario.

2. The civil aircraft is being continuously illuminated by the mainbeam of the emitting antenna.

3. All calculations consider only free-space loss between the emitter and the aircraft. Above 30 MHz, no consideration is given to reflecting surfaces or obstacles that may exist in the vicinity of either the emitter or the aircraft. Below 30 MHz, only the ground reflected wave is considered and assumed to combine constructively with the direct wave, effectively doubling the field strength.

4. Field strength calculations for aircraft locations within the near field of the emitting antenna are made using the near-field correction factors discussed later in this paper.

5. The resulting field strength is independent of modulation or any other equipment-related factor.

6. The cumulative effect of two or more emitters illuminating the aircraft is not considered.

### DETERMINATION OF THE MINIMUM DISTANCES FOR THE WORST-CASE TOTAL ENVIRONMENT SCENARIO

The total environment can be separated into four parts: the airport environment, the aircraft-to-aircraft environment, the ground environment, and the shipboard environment. While on the ground, the aircraft will be exposed to emitters in the airport environment. While in flight, the aircraft will encounter emitters in the aircraft-to-aircraft, ground, and shipboard environments. The minimum distance for an aircraft in one of these environments is defined as the closest the aircraft can approach an emitter in that environment. Each environment and its minimum separation distance will be discussed in turn. The minimum distances are summarized in table A-1.

TABLE A-1. SUMMARY OF MINIMUM DISTANCES FOR THE WORST-CASE SCENARIO

| ENVIRONMENT | MINIMUM DISTANCE |
|---|---|
| FIXED EMITTERS ON AIRPORT | 250 FT |
| MOBILE EMITTERS ON AIRPORT | 50 FT |
| INTERCEPTOR AIRCRAFT EMITTERS | 50 FT |
| NON-INTERCEPTOR AIRCRAFT EMITTERS | 500 FT |
| GENERAL GROUND EMITTERS | 500 FT |
| SHIPBOARD EMITTERS | 300 FT |

## The Airport Environment

The airport environment consists of fixed and mobile emitters located on an airport. For this discussion, the airport includes an area defined by a five-nautical-mile radius from the geographic center of the airport. The minimum distance at which field strengths are to be calculated differs for fixed and mobile emitters.

Fixed Emitters. The fixed airport environment consists of all fixed emitters located on an airport. In general, the minimum distance between a fixed emitter and the taxiway or runway is defined by regulations. This minimum distance is used as the minimum separation distance between the aircraft and the fixed airport environment.

Table A-2 lists the typical fixed emitters in the U.S. airport environment. Not all of these emitters are located on every airport, but they are located on some airport in the United States. Based on FAA regulations, fixed emitters are located no closer to an airport runway or taxiway than 250 ft. A minimum distance of 250 ft, therefore, was used in the calculation of the field strengths from the fixed emitters on a U.S. airport.

Mobile Emitters. The mobile airport environment consists of all emitters that are not in a fixed location. Emitters, such as commercial VHF radios on ground support vehicles, are part of the mobile environment. Emitters, such as HF and UHF communications, TACAN, Doppler Navigation Radars, radio altimeters, aircraft weather radars, and ATCRBS beacons, aboard other aircraft are also included in the mobile airport environment. These aircraft emitters may be operating while the aircraft is on the ground and waiting to take off.

A minimum distance of 50 ft was used in calculating field strengths from mobile emitters on the airports in the U.S. analysis.

TABLE A-2. TYPICAL FIXED AIRPORT ENVIRONMENTAL EMITTERS

| |
|---|
| MARKER BEACON |
| LOCALIZER |
| VOR |
| GLIDE SLOPE |
| GROUND CONTROLLED APPROACH RADAR |
| DISTANCE MEASURING EQUIPMENT |
| TACAN |
| MICROWAVE LANDING SYSTEM |
| AIRPORT SURVEILLANCE RADAR |
| AIR ROUTE SURVEILLANCE RADAR |
| WEATHER RADAR |
| ATCRBS INTERROGATOR |
| VHF AND UHF COMMUNICATION AND TELEMETRY |

### Aircraft-to-Aircraft Environment

This environment consists of emitters onboard other aircraft at distances much closer than normal in-flight separation. Note that the emitters on other civil aircraft were included in the mobile airport environment. Therefore, only military aircraft need to be considered in this environment.

The military aircraft fall into two categories: interceptor and noninterceptor aircraft. An interceptor aircraft may approach as close as 50 ft to an unidentified commercial aircraft while attempting to establish the identity of, and provide instructions to, the aircraft. It can be assumed that very high powered military emitters such as electronic countermeasure (ECM) systems will not be operating at this close range. Noninterceptor aircraft would not intentionally approach closer than 500 ft from another aircraft but may be operating high powered emitters such as early warning radars and ECM systems. In the U.S. study, ECAC used these distances when calculating electric field strengths.

### Ground Environment

Of the four environments, the ground environment is the largest since it includes all fixed and ground mobile emitters that are not located on airports. Emitters such as sounders, troposcatter communications, commercial broadcast, radar astronomy, land mobile, test and training equipment, radars and transmitting earth terminals are part of the ground environment.

The International Civil Aviation Organization (ICAO) aircraft minimum obstruction clearance is 500 ft above ground level. Therefore, the minimum distance at which field strengths are calculated is 500 ft. Note that for most high power emitters, this places the aircraft within the near field of the emitting antenna.

Shipboard Environment

This environment includes emitters on commercial and military ships that may be located in harbors near airports. Some of the high-powered emitters that are included are: search and track radars, fire control radars, satellite communications, HF communications, and electronic countermeasure systems. A minimum distance of 1000 ft was used in the U.S. analysis based on the locations of U.S. harbors.

DETERMINATION OF THE MINIMUM DISTANCES FOR THE TAKEOFF AND LANDING SCENARIO

The takeoff and landing scenario is concerned with the environment on and around airports, where the aircraft is expected to be near the ground. The worst-case condition is the one-engine out situation for a two engine aircraft. In this situation, the aircraft must climb to a minimum altitude and must maintain that altitude. Figure A-1 shows the FAA criteria and the minimum altitudes that the aircraft must maintain. Based on this criteria, the minimum distances for field-strength calculations are as follows:

1. While on the airport runways or taxiways, the minimum distance is 250 ft, as discussed under the airport environment section, above.

2. The aircraft must be at an altitude of 35 ft at threshold (end of runway), climbing at a minimum gradient of 2.4%. This places the aircraft at an altitude of 300 ft at a distance of 1.84 nautical miles from the end of the runway.

3. The aircraft will be at an altitude of 300 ft to a distance of 4.5 nmi from the end of the runway.

4. At 4.5 nmi, the minimum altitude is specified as 500 ft.

5. The minimum distance between an aircraft and an emitter is dependent on the location of the emitter and the altitude at that location as given in 1 through 4 above. Where appropriate, the height of the emitting antenna above ground should be deducted from the minimum aircraft altitude to obtain the minimum distance from that specific emitter.

CALCULATION OF FIELD STRENGTHS

The conventional measure of the intensity of a radiated electromagnetic wave is a measure of the intensity of the electric field in volts per meter. (Note that the distances in the above discussion were in English units since this is common for the aviation industry. The discussion of electric field strengths will be in metric units with volts per meter being the unit used in international regulations.) The field intensity of a radiated wave in free space falls off in direct proportion to the distance from the transmitting antenna. For practical purposes free space propagation is realized if the following conditions are fulfilled: No large obstacles intervene between the antenna and the aircraft along an optical line of sight; no alternate transmission path can be followed by a substantial fraction of the radiated energy (this is the same as Assumption 3 in the Introduction section); the intervening atmosphere has a constant index of refraction, so that no bending of the wave occurs; and the intervening atmosphere does not absorb energy from the wave at the frequency used. For this analysis, it is assumed that these conditions are fulfilled between an emitter in the environment and an aircraft.

The emitter antenna will be either an aperture, phased array or linear antenna. Phased array antennas are assumed to have similar radiating properties to an aperture antenna of the same physical dimensions. Elliptical antennas are approximated by rectangular antennas for these calculations.

Calculation of Field Strengths in the Far Field

Aperture Antennas. The power density obeys the inverse square law starting at a certain distance from the antenna where the antenna appears to be a point source. This is where the "Fraunhofer Region," or far field, begins. The distance to the far-field boundary for aperture antennas can be designated as:

$$D_f = 2\,L^2/\lambda \qquad (1)$$

where:

$D_f$ - distance to the far-field boundary, meters

L - Maximum dimension of antenna, meters

$\lambda$ - wavelength, meters

In the Fraunhofer Region, the radiation is in a diverging beam shape, where the intensity is maximum at the beam center, and decreases away from the beam center as the angle of divergence increases. If the antenna is made larger or the antenna illumination is made more uniform, the radiated beam is made narrower and the beam center power density is made higher. The power density at the beam center in the far field is given by the equation:

$$P_D = \frac{PG}{4\pi d^2} \qquad (2)$$

where:

$P_D$ - power density, watts/meter$^2$

P - transmitter power, watts

G - transmitter antenna gain, unitless

d - distance, meters

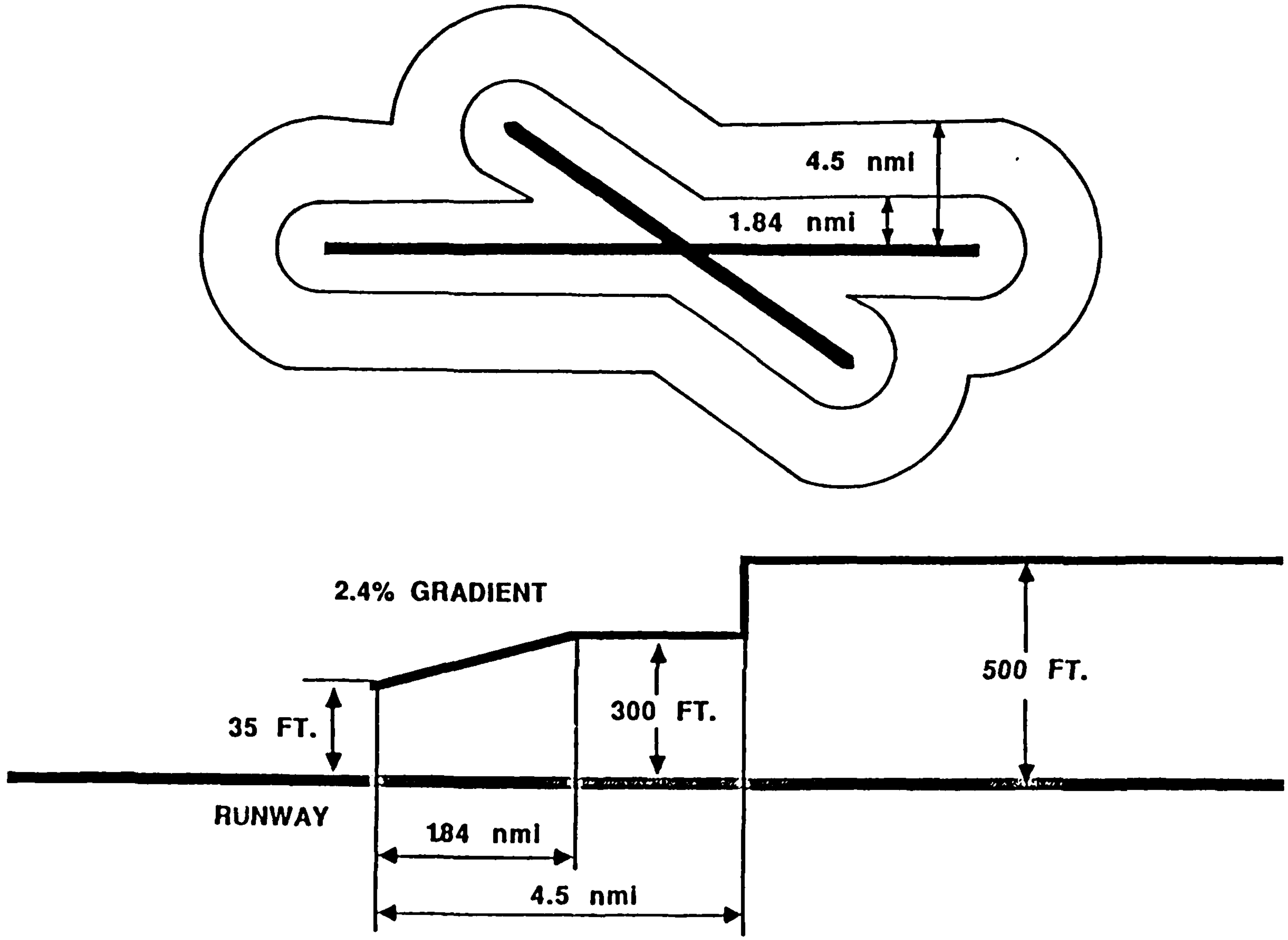


FIGURE A-1. FAA CRITERIA FOR A ONE-ENGINE OUT SITUATION FOR A TWO-ENGINE AIRPLANE

Power density is converted to field strength (FS) using the impedance of free space in Equation 3:

$$FS = \sqrt{P_D(377)} \tag{3}$$

Linear Antennas. Equations 2 and 3 can be used to calculate the electric field strength at given distances from a linear emitting antenna. The far-field boundary is designated as $4\lambda$.

Calculation of Field Strengths in the Near Field

Power densities in the near field are calculated using the far-field equation (Equation 2) and a near-field gain reduction factor ($\chi$), or:

$$P_D = \frac{PG\chi}{4\pi d^2} \tag{4}$$

where all values are previously defined. Power density is converted to field strength using Equation 3.

The near field is the region within the far-field boundary, as defined by Equation 1 for aperture antennas and by $4\lambda$ for linear antennas. It should be noted that for the aircraft environment scenarios described above the aircraft is within the near field of most emitters using aperture antennas and in the far field for all of the emitters using linear antennas.

Near field gain reduction factors were calculated for the ECAC study using US Department of Defense approved techniques. A summary of these techniques for aperture antennas is presented below. No near field gain reduction techniques are required for linear antennas.

Near-field Gain Reduction for Rectangular Aperture Antennas. For rectangular aperture antennas the vertical and horizontal axis may not have the same illumination taper. Therefore, the gain reduction for each axis must be determined, then summed (in dB) to determine the total gain reduction.

Using the antenna axial illuminations, the main beam axis near-field gain reduction for a selected distance, d, from the antenna may be determined in the following manner:

1. Normalize the selected distance:

$$\Delta_h = d/(L_h^2 /\lambda)$$

and (5)

$$\Delta_v = d/(L_v^2 /\lambda)$$

where:

$\Delta_v$, $\Delta_h$ - normalized distance associated with vertical and horizontal antenna dimensions, respectively.

2. From table A-3, find the near-field gain reduction factors ($\chi_h$ and $\chi_v$) using the axis illuminations and the $\Delta$ values. The total near-field gain reduction is the sum of the gain reductions, in dB, converted to absolute form:

$$\chi = 10^{-[(\chi_h + \chi_v)/10]} \tag{6}$$

TABLE A-3. NEAR-FIELD CORRECTION FACTOR FOR RECTANGULAR APERTURE ANTENNAS

| FOR UNIFORM ILLUMINATION | | $\chi$, dB FOR ALL OTHER ILLUMINATIONS | | | | |
|---|---|---|---|---|---|---|
| $\Delta$ | $\chi$, dB | $\Delta$ | cos | cos$^2$ | cos$^3$ | cos$^4$ |
| 0.016 | 17.50 | 0.010 | ---- | 14.0 | 12.6 | 11.5 |
| 0.020 | 17.25 | 0.015 | 14.0 | 12.4 | 11.0 | 9.8 |
| 0.021 | 15.95 | 0.020 | 13.2 | 11.2 | 9.7 | 8.6 |
| 0.023 | 16.75 | 0.025 | 12.2 | 10.2 | 8.8 | 7.8 |
| 0.026 | 14.75 | 0.030 | 11.4 | 9.5 | 8.0 | 7.0 |
| 0.032 | 15.65 | 0.035 | 10.8 | 8.8 | 7.4 | 6.4 |
| 0.037 | 13.50 | 0.040 | 10.2 | 8.2 | 6.8 | 5.8 |
| 0.042 | 15.00 | 0.050 | 9.2 | 7.2 | 5.8 | 4.8 |
| 0.056 | 11.95 | 0.060 | 8.4 | 6.6 | 5.0 | 4.0 |
| 0.065 | 13.10 | 0.070 | 7.6 | 5.8 | 4.4 | 3.4 |
| 0.093 | 9.0 | 0.080 | 7.0 | 5.3 | 3.8 | 2.8 |
| 0.14 | 11.0 | 0.090 | 6.6 | 4.7 | 3.4 | 2.4 |
| 0.4 | 2.2 | 0.10 | 6.1 | 4.2 | 3.0 | 2.1 |
| 1.0 | 0.3 | 0.15 | 4.3 | 2.6 | 1.6 | 1.2 |
| | | 0.20 | 3.0 | 1.6 | 0.9 | 0.6 |
| | | 0.25 | 2.0 | 1.1 | 0.6 | 0.4 |
| | | 0.30 | 1.5 | 0.8 | 0.4 | 0.3 |
| | | 0.35 | 1.1 | 0.6 | 0.2 | 0.2 |
| | | 0.40 | 0.8 | 0.4 | 0.2 | 0.2 |
| | | 0.50 | 0.5 | 0.2 | 0 | 0 |
| | | 0.60 | 0.4 | 0.2 | 0 | 0 |
| | | 0.70 | 0.2 | 0.1 | 0 | 0 |
| | | 0.80 | 0.2 | 0 | 0 | 0 |
| | | 0.9 | 0.1 | 0 | 0 | 0 |
| | | 1.0 | 0 | 0 | 0 | 0 |

NOTE: If the value of $\Delta$ falls between two points on the chart, then the value of $\chi$ should be interpolated.

3. Multiply the power density at distance, d, obtained using Equation 2, by $\chi$ as shown in Equation 4. Use Equation 3 to obtain the field strength from $P_D$.

Near-field Gain Reduction for Circular Aperture Antennas. The method employed with the near-field gain reduction factor for circular antennas is different than that for rectangular antennas. The axial power density at a given distance, d, from a circular aperture antenna is determined as follows:

1. Calculate the reference power density by substituting $2L^2/\lambda$ for distance in Equation 2. Or:

$$P_{D_0} = \frac{PG\lambda^2}{16\pi L^4} \tag{7}$$

where:

$P_{D_0}$ - reference power density, W/m$^2$

2. Convert distance, d, to normalized distance $\Delta = d\lambda/2L^2$.

3. Using the antenna illumination, obtain the value of $\chi$, the near-field gain reduction value, from table A-4, and multiply it by the reference power density to obtain the corrected power density. That is:

$$P_D = \chi P_{D_0} \tag{8}$$

4. Convert to field strength using Equation 3.

## DEFINING AND DETERMINING THE VALUES OF NECESSARY PARAMETERS

The methodology for field strength calculations, discussed above, is dependent on the availability of technical information on the emitters. Specifically, the calculations require the following technical parameters: transmitter power, wavelength, antenna gain, antenna dimensions, and antenna beamwidths. These parameters are discussed below along with techniques for estimating parameter values if they are not available.

### Peak Power

The peak power is used in calculating the peak field strength from the emitter. It is usually recorded as the maximum rated power at the output of the emitter before the antenna connections. It does not include system losses or losses due to equipment aging. If the peak power is not available, then no calculations can be made.

TABLE A-4. NEAR-FIELD CORRECTION FACTOR FOR CIRCULAR APERTURE ANTENNAS

| | $\chi$ FOR ALL ILLUMINATIONS[1,2] | | | |
|---|---|---|---|---|
| $\Delta$ | UNIFORM | $(1-r^2)$ | $(1-r^2)^2$ | $(1-r^2)^3$ |
| 0.01 | 26.0 | 27.7 | 59.0 | 103.5 |
| 0.02 | 26.0 | 28.1 | 59.2 | 102.5 |
| 0.03 | 26.0 | 30.1 | 59.4 | 102.0 |
| 0.04 | 26.0 | 31.9 | 59.7 | 102.0 |
| 0.05 | 26.0 | 33.5 | 60.7 | 101.0 |
| 0.06 | 26.0 | 35.0 | 62.6 | 98.0 |
| 0.07 | 26.0 | 37.0 | 63.7 | 92.0 |
| 0.08 | 26.0 | 39.0 | 63.5 | 84.0 |
| 0.09 | 26.0 | 40.0 | 61.0 | 77.0 |
| 0.1 | 26.0 | 40.7 | 56.0 | 69.0 |
| 0.15 | 24.5 | 29.0 | 32.0 | 35.0 |
| 0.2 | 18.0 | 19.5 | 20.1 | 22.0 |
| 0.3 | 9.5 | 10.5 | 10.5 | 11.0 |
| 0.4 | 5.5 | 6.0 | 6.0 | 6.0 |
| 0.5 | 3.5 | 3.9 | 3.9 | 3.5 |

NOTES:

1. If the value of $\Delta$ falls between two points on the chart, then the value of $\chi$ should be interpolated.
2. For $\Delta > 0.5$, calculate field strengths using the far-field equation.

Average Power

The average field strength from the emitter is calculated from the average output power of the emitter. This is the maximum rated average power before the antenna connections. If this value is not available for a particular emitter, it can be calculated from the peak power and other parameters.

The average power is the product of the peak power and duty cycle. The duty cycle is a unitless number, less than or equal to 1.0, which is the product of the pulsewidth (PW) in seconds and the pulse repetition frequency (PRF) in Hertz. Emitter documentation often lists multiple values of PW and PRF or the PW and PRF as ranges. The duty cycle may be the product of some PW and some PRF in the range(s) but not necessarily the maximum value(s). If the precise duty cycle cannot be determined, then the maximum values may be used to obtain a conservative estimate of the duty cycle. For non-pulsed systems, the duty cycle is unity and the peak and average powers are the same.

Maximum Mainbeam Antenna Gain

As mentioned above, it is assumed that the aircraft is within the mainbeam of the emitting antenna for the purpose of calculating field strength. The mainbeam gain is the maximum possible gain of the antenna. If the gain is not available, it can be calculated from the area of the antenna aperture, the beamwidths, and the antenna illumination. The following procedures will show how to derive the antenna gain from one or more of these factors.

Calculating Gain of Aperture Antennas if Antenna Dimensions Are Known. If the dimensions of the antenna are known, then the gain can be calculated by application of some simplifying assumptions. Equation 9 is the basic formula for calculating gain:

$$G = \frac{4\pi^2 A\rho}{\lambda^2} \qquad (9)$$

where:

G - gain, unitless

A - area of antenna aperture, square meters

$\rho$ - antenna efficiency, unitless

F - Antenna gain factor, unitless

$\lambda$ - wavelength, meters

The antenna efficiency is a rating of how well the antenna emits the input power. Antenna efficiency is usually between 0.5 and 0.9, with a typical value of 0.55. If no other information is available, the typical value of 0.55 will be used for $\rho$. The product of antenna aperture and efficiency is known as the effective aperture, $A_e$, of the antenna. The antenna factor, F, is dependent on the type of aperture illumination used. If the aperture illumination is not known, uniform aperture illumination will be used because it will produce a conservative value of gain., For uniform illumination, F = 1.

Calculating Gain if Antenna Beamwidths Are Known. An approximation of gain from the known values of the horizontal and vertical beamwidths is:

$$G \approx \frac{20{,}000}{\theta_h \theta_v}$$

where:

$\theta_h, \theta_v$ - horizontal and vertical beamwidths, degrees

This assumes that the illumination is uniform and the antenna efficiency is 0.55.

Calculating Gain if Antenna Beamwidths and Dimensions Are Known. If the antenna dimensions and beamwidths are known, a more precise value for gain can be calculated. Assume an antenna efficiency of 0.55. Calculate the antenna aperture area. Then determine the gain factor from table A-5 for rectangular apertures and table A-6 for circular apertures. Substitute these values into Equation 9.

To determine the gain factor for rectangular apertures:

1. Use table A-5. Note that the horizontal illumination may be different than the vertical illumination, with a different gain factor for each dimension.

2. Observe between what values $\theta_h$ falls after substituting the appropriate values of $L_h$ and wavelength.

3. Find the gain factor, $F_h$, from the table.

4. Repeat steps 2 and 3 for $\theta_v$ and $L_v$ to obtain $F_v$.

5. Obtain the gain factor for the antenna from the product of the horizontal and vertical gain factors. That is, $F = F_h F_v$.

For circular apertures:

1. Use table A-6.

2. Observe the range of values of $\theta$ after substituting the appropriate values for diameter and wavelength.

3. Find the gain factor, F; from the table.

Calculating Gain if Antenna Illumination is Known. By itself, antenna illumination can only determine the gain factor (F). Either beamwidth or antenna dimension (for each axis, if the aperture is rectangular) is also required to calculate gain using the above procedure. Only one of the parameters is required because the other parameter can be derived using tables A-5 and A-6.

If all three parameters (i.e., illumination, beamwidths and dimensions) are known, then:

1. The Gain Factor(s) can be obtained using table A-5 or A-6.

2. Calculate $\theta$ using the formulas in the last column of the selected table and compare with the actual beamwidth(s). If the corresponding information does not agree, further checking on the available technical parameters may be required.

TABLE A-5. BEAMWIDTHS AND GAIN FACTORS OF RECTANGULAR ANTENNAS WITH VARIOUS ILLUMINATIONS

| ILLUMINATIONS | GAIN FACTOR, F | $\theta$, DEGREES |
|---|---|---|
| Uniform | 1.00 | $50.4\lambda/L$ to $68.7\lambda/L$ |
| Cosine | 0.81 | $68.7\lambda/L$ to $83.0\lambda/L$ |
| Cosine Squared | 0.667 | $83.0\lambda/L$ to $95.0\lambda/L$ |
| Cosine Cubed | 0.575 | $95.0\lambda/L$ to $110\lambda/L$ |
| Cosine Fourth | 0.515 | $110\lambda/L$ to $116\lambda/L$ |

TABLE A-6. BEAMWIDTHS AND GAIN FACTORS OF CIRCULAR ANTENNAS WITH VARIOUS ILLUMINATIONS

| ILLUMINATIONS | GAIN FACTOR, F | $\theta$, DEGREES |
|---|---|---|
| Uniform | 1.00 | $58.5\lambda/L$ to $72.8\lambda/L$ |
| $(1-r^2)$ | 0.75 | $72.8\lambda/L$ to $84.2\lambda/L$ |
| $(1-r^2)^2$ | 0.56 | $84.2\lambda/L$ to $94.5\lambda/L$ |
| $(1-r^2)^3$ | 0.44 | $94.5\lambda/L$ to $103.5\lambda/L$ |
| Cosine Fourth | 0.515 | $110\lambda/L$ to $116\lambda/L$ |

Median Gain. The median gain is sometimes used instead of mainbeam gain when calculating field strengths if antenna rotation is a factor. The median gain is the gain averaged over the entire rotation. Usually, median gain is used if an object if in the mainbeam of the antenna for too short a period of time. Yet, an aircraft may be in the mainbeam of the antenna for sufficient time to degrade or damage sensitive flight-critical systems aboard the aircraft. For example, an aircraft approaching for a landing at a typical velocity of 170 nautical miles per hour in the same direction that an antenna for an air search radar is rotating at a typical rate of 10 rotations per minute will be in the mainbeam of the antenna for one second. Damage to electronic equipment can occur during exposures of a few milliseconds. It is, therefore, recommended that mainbeam gain be used in field strength calculations instead of median gain.

## Beamwidths and Antenna Dimensions

Beamwidths. In and of itself, beamwidths are not directly necessary for the calculation of field strengths, yet beamwidths serve to check or derive a value for gain, and to derive a value for antenna dimension.

Antenna Dimensions. The antenna length and width for rectangular apertures ($L_h$ and $L_v$), or diameter (L) for circular apertures is required in the calculation of field strength in the near field. Given that gain is known, the antenna dimension can be calculated based on specific assumptions. Fewer assumptions are required if more information about the antenna is known.

If only the gain is known: assume $F = 1$ and $\rho = 0.55$. Solve Equation 9 for A, the antenna aperture area. Now assume a circular aperture and derive the diameter. The diameter is the dimension used in field strength calculations.

If the horizontal and vertical beamwidths are also knows: assume uniform illumination for each axis. For rectangular aperture antennas, derive the value of $L_h$ and $L_v$ using table A-5. For circular aperture antennas, derive a value of L from table A-6. Substitute the appropriate values of F and A into Equation 9 and derive the efficiency, $\rho$. If the efficiency is not between 0.5 and 0.9, repeat these steps with a different assumption for illumination (one or both axis for rectangular apertures) until the efficiency condition is met.

If beamwidths and illuminations are known: Derive the value(s) of L from table A-5 or A-6. Substitute the appropriate values of F and A into Equation 9 and derive the efficiency. If the efficiency is not between 0.5 and 0.9, check the values of the parameters for correctness.

## Peak and Average Field Strength Predictions

Using the methods described above, the electric field strengths can be calculated from the data collected on the emitters in a particular environment. The distance at which the field strengths are to be calculated is dependent on the environment in question. A separate set of results for each of the environments discussed above is recommended. Using peak power, the maximum peak field strengths can be calculated for the emitters. Average transmitted power is used to calculate the maximum average electric field strength. The resultant electric field strength predictions can be tabulated in preparation for producing envelope graphs.

## PRESENTATION OF RESULTS

The most convenient method of presenting the maximum electric field strength predictions is in the form of envelope graphs. First, the results of the analysis are plotted on log-log paper. The abscissa is frequency from 10 kHz to 100 GHz. The ordinate is field strength in volts per meter (V/m) with a range from 1 V/m to some power of 10 that is greater than the greatest value to be plotted on the graph. The resultant graph is a histogram. An example of a histogram is given in figure A-2. (Note that the value plotted in figures A-2 through A-6 and table A-7 are random and are merely used for illustration purposes.)

The "envelope" of the graph is a discontinuous line that identifies the level at which all of the values on the graph are beneath. The data in figure A-2 with an envelope over it is shown in figure A-3. Figure A-4 is just the envelope of the values. As can be seen, the values that produced the electric field strength envelope cannot be determined from figure A-4. The values of the levels in the envelope graphs are shown in table A-7. Note that such tables are required for the establishment of an international standard.

The results of both the total environment analysis and the takeoff and landing analysis is a composite of several environments. The composite graph merely follows the maximum value of the component envelope graphs. For example, the envelope graph of figure A-4 is combined with the envelope graph of figure A-5 to produce the composite graph is figure A-6. For the total environment, as many as 12 envelope graphs are produced and combined into two composite graphs, one for peak and one for average field strength. For the takeoff and landing environment, two graphs for the environments around each of the airports are produced. In the U.S. case, six airports were examined resulting in 12 graphs. The two composite graphs that are produced for the takeoff and landing scenario are comprised of these 12 individual graphs.

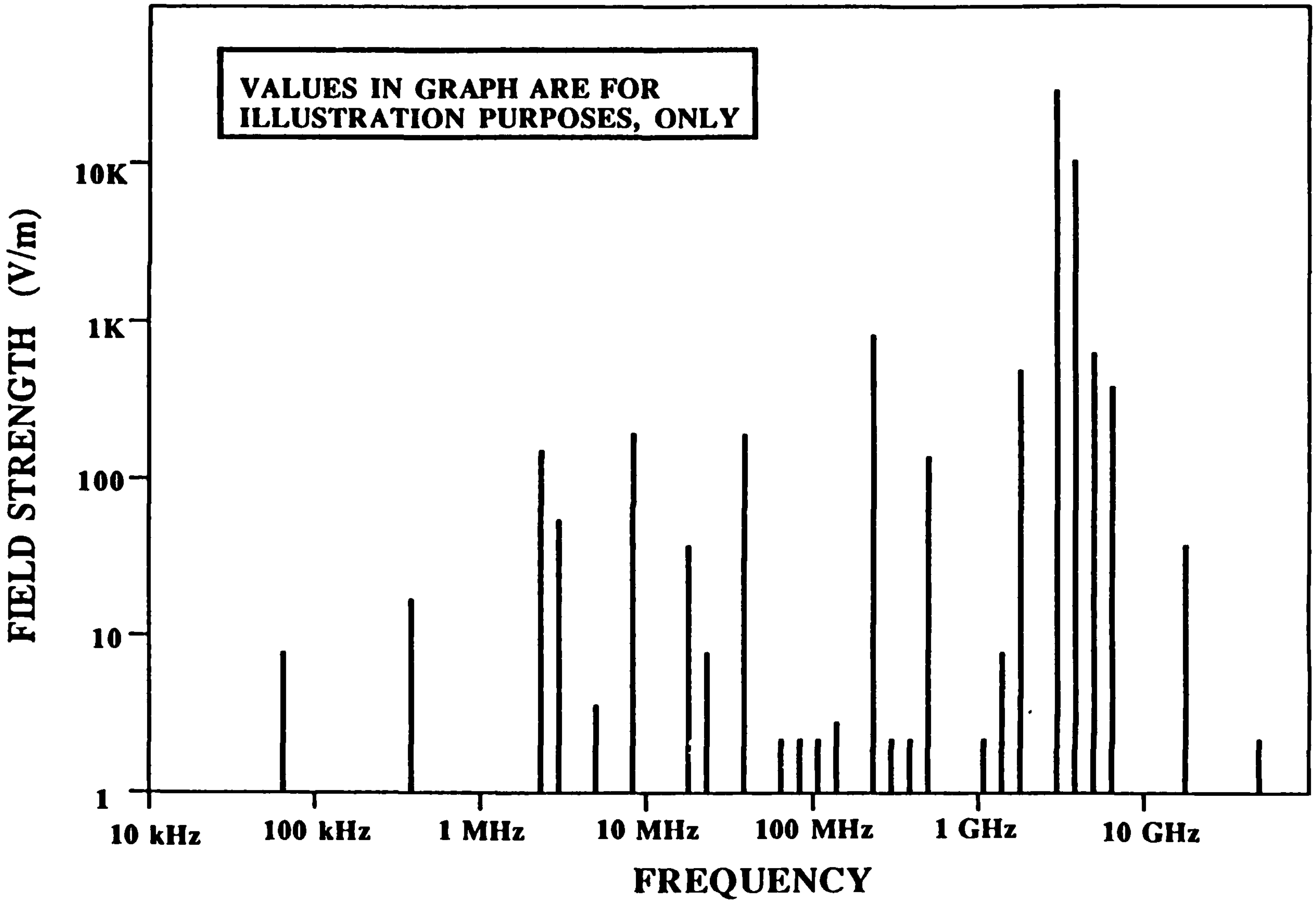


FIGURE A-2. EXAMPLE OF ELECTRIC FIELD STRENGTH VERSUS FREQUENCY GRAPH ON A LOG-LOG SCALE

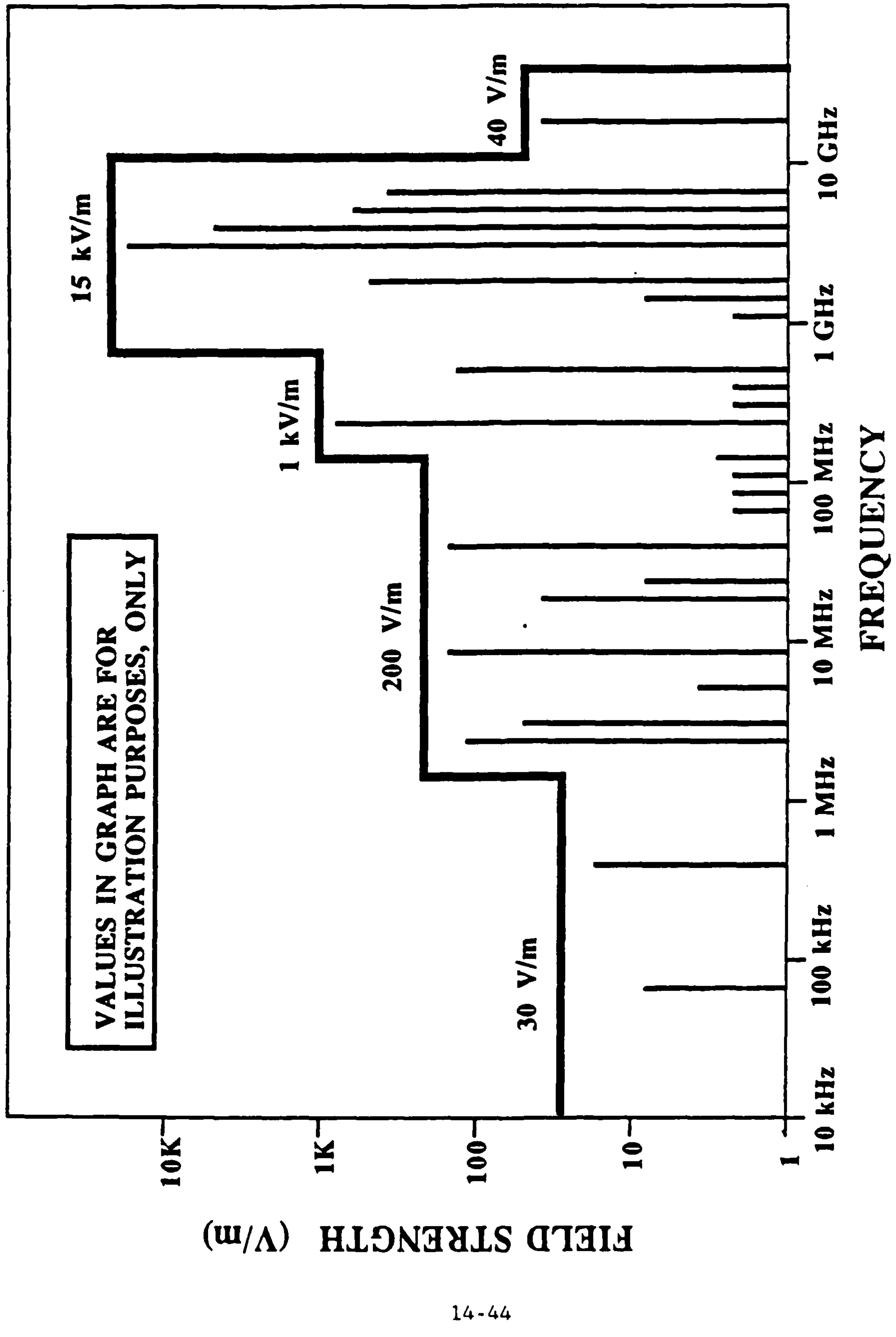


FIGURE A-3. EXAMPLE OF ENVELOPE OF FIELD STRENGTH VERSUS FREQUENCY GRAPH

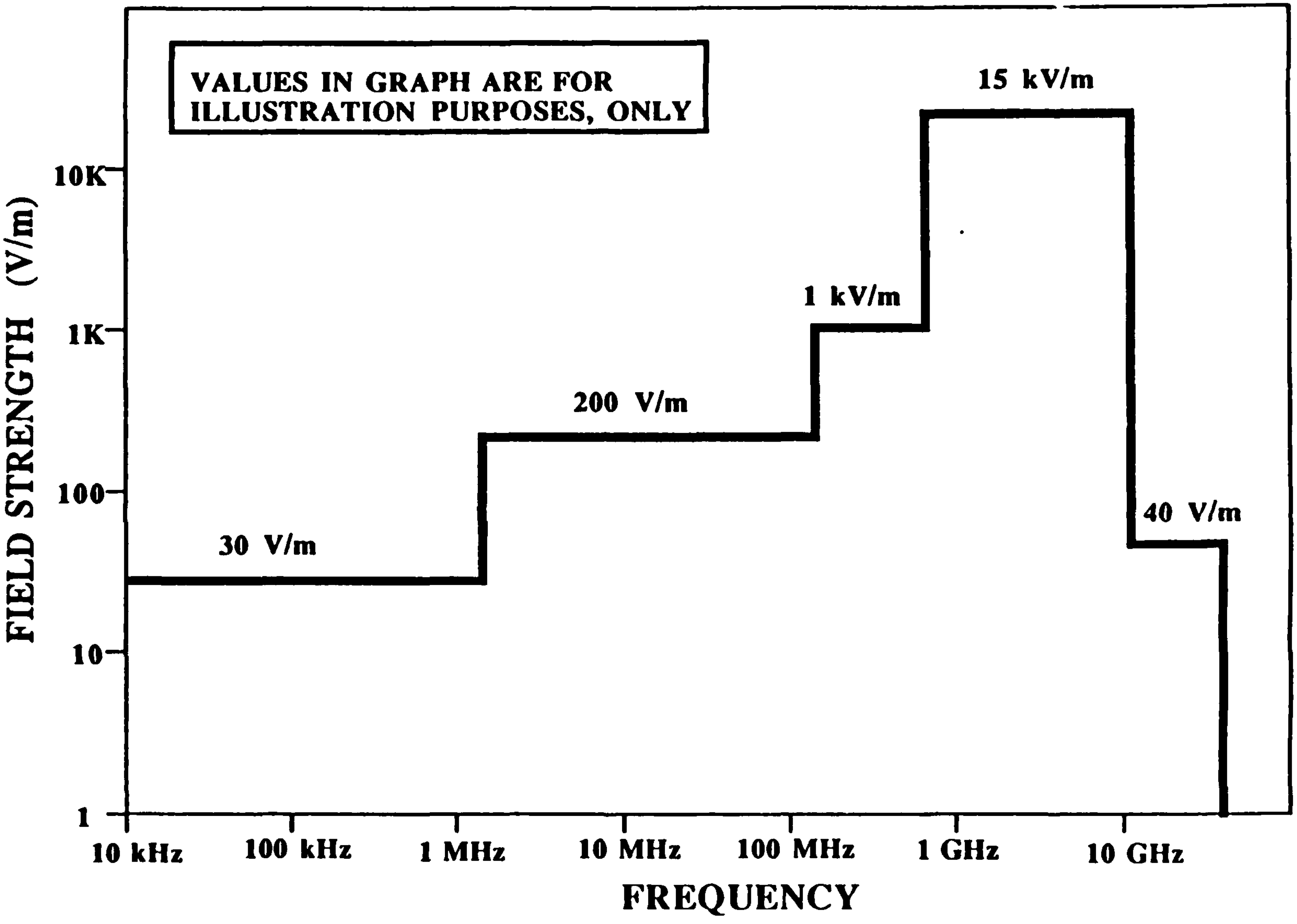


FIGURE A-4. EXAMPLE OF FINAL OUTPUT

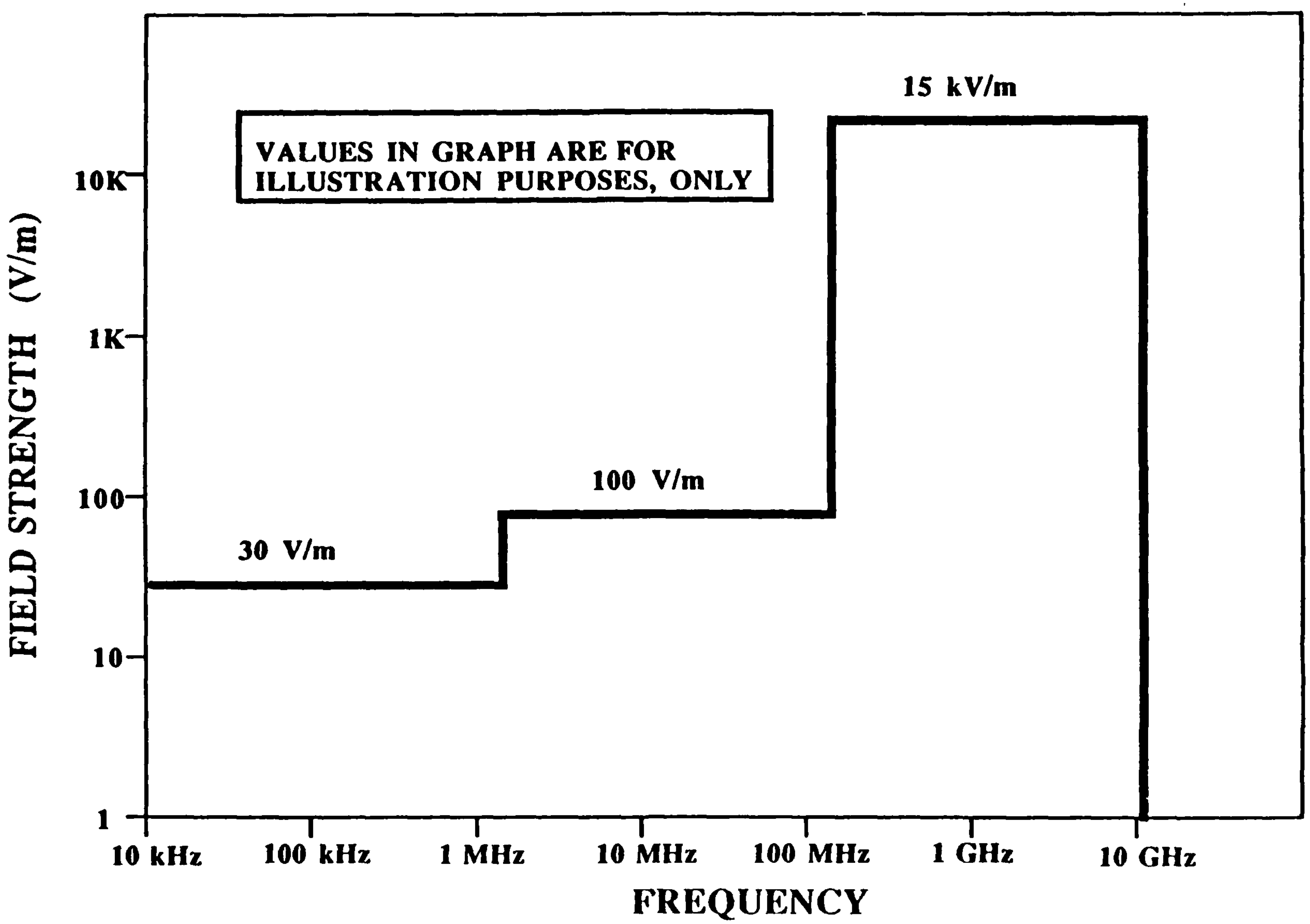


FIGURE A-5. EXAMPLE OF ENVELOPE GRAPH OF A SECOND ENVIRONMENT, TO BE COMBINED WITH FIGURE A-4 TO FORM A COMPOSITE GRAPH

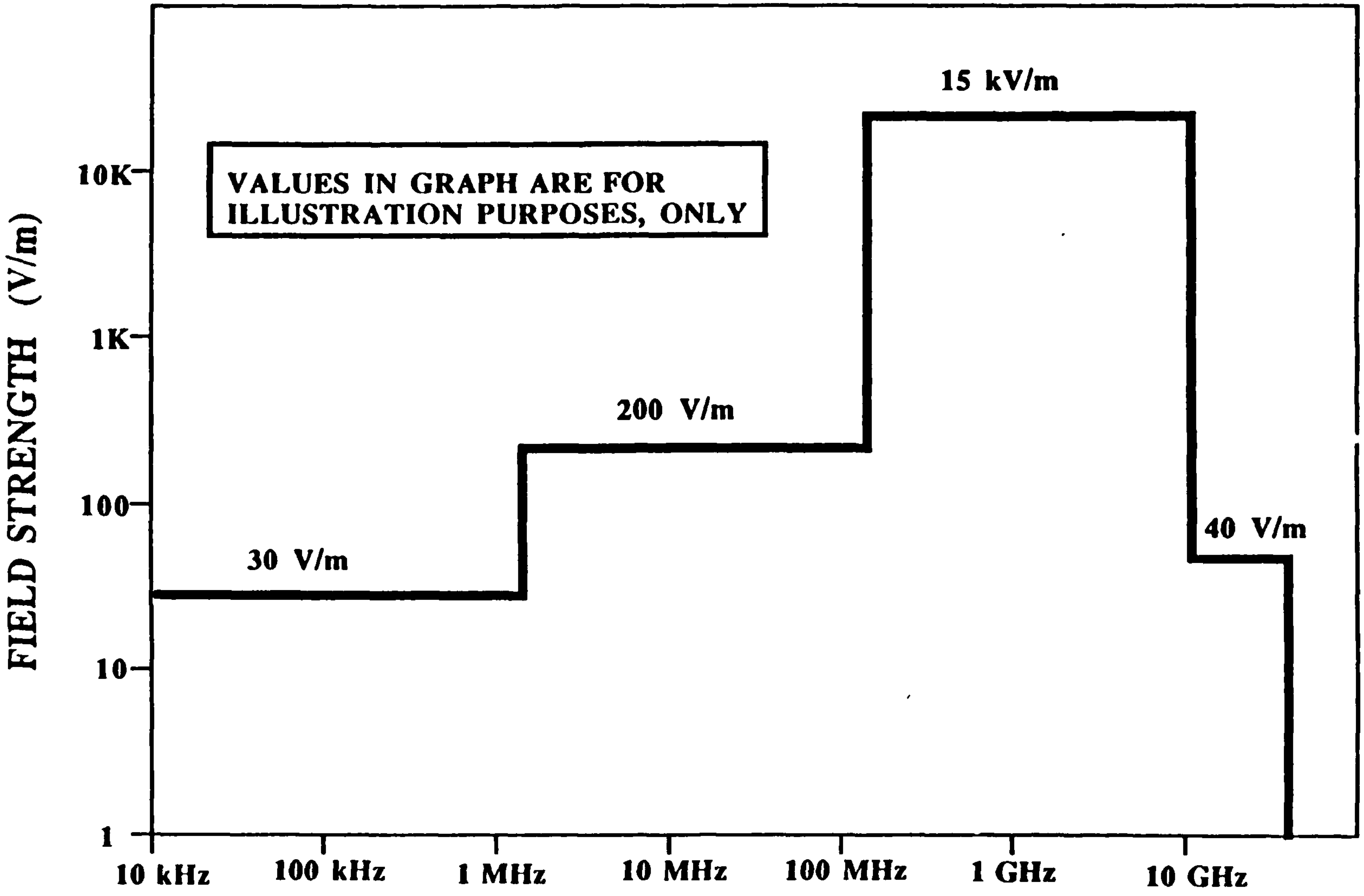


FIGURE A-6. COMPOSITE OF TWO ENVIRONMENTS SHOWN IN FIGURES A-4 AND A-5

TABLE A-7. SAMPLE ELECTRIC FIELD STRENGTH LEVELS USING VALUES IN FIGURE A-4

| FREQUENCY | FIELD STRENGTH (V/m) |
|---|---|
| 10 kHz - 2 MHz | 30 |
| 2 MHz - 100 MHz | 200 |
| 100 MHz - 800 MHz | 1000 |
| 800 MHz - 10 GHz | 15,000 |
| 10 GHz - 40 GHz | 40 |

NOTE: Values in table are for illustrative purposes, only.

## SUMMARY

The intention of this chapter was to provide the guidelines that were used to calculate the maximum electromagnetic radiation level that would be experienced by an aircraft flying in the United States. These guidelines are presented in an effort to promote uniformity of results from other members of the international aviation community in order that all results can be combined and used to develop an international RF susceptibility standard. Two aircraft scenarios were discussed: a worst-case scenario and a takeoff and landing scenario. The logic used by the United States to develop minimum distance criteria for each scenario was presented. The techniques used to calculate the far field and near field electric field strengths were described. Emitter parameters and methods that can be used to estimate values for parameters that are not available were discussed. Finally, how to present the results in the form of envelope graphs (useful because the results can be displayed in a simple chart without identifying the emitters involved) and field strength tables was shown.

# BIBLIOGRAPHY

DOD/ECAC, Guidelines for Developing Maximum Peak and Average Field Strength Envelope Graphs for Aircraft, Sept. 1987.

MAC Test 15-117-87, Electromagnetic Radiation Measurement, 7 June 1988.

MIL-STD-235-1A, Electromagnetic (Radiated) Environment Considerations for Design and Procurement of Electrical and Electronic Equipment.

MIL-STD-461B, Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference.

MIL-STD-462, Measurement of Electromagnetic Interference Characteristics.

RTCA DO-160B, Environmental Conditions and Test Procedures for Airborne Equipment.

# LIST OF ACRONYMS

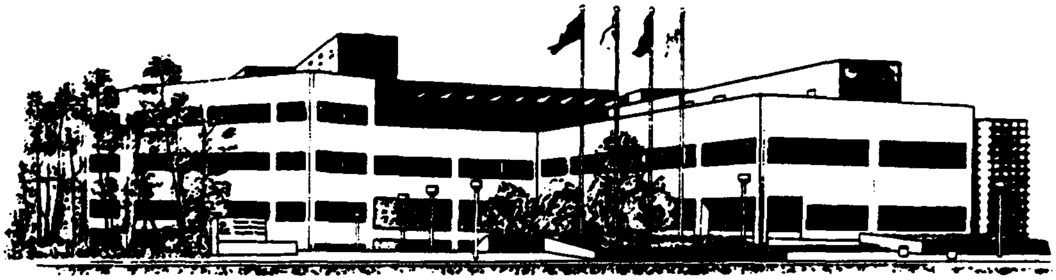
| | |
|---|---|
| AC | Advisory Circular |
| AM | Amplitude Modulation |
| ATCRBS | Air Traffic Control Radar Beacon System |
| AWACS | Airborne Warning and Control System |
| CAA | Civil Aviation Authority |
| CONUS | Contiguous United States |
| dBi | Decibels with respect to one milliampere |
| DGAC | Directorate Generale Aviation Civile |
| DOD | Department of Defense |
| ECAC | Electromagnetic Compatibility Analysis Center |
| ECM | Electronic Counter Measures |
| EMC | Electromagnetic Compatibility |
| EME | Electromagnetic Environment |
| EMR | Electromagnetic Radiation |
| EUROCAE | European Organization for Civil Aviation Electronics |
| FAA | Federal Aviation Administration |
| FM | Frequency Modulation |
| ft | feet |
| HF | High Frequency |
| HERF | High Energy Radio Frequency |
| ICAO | International Civil Aviation Organization |
| IFF | Identify Friend or Foe |
| kHz | kilohertz |
| MHz | megahertz |
| NATO | North Atlantic Treaty Organization |
| nmi | nautical mile |
| NPRM | Notice of Proposed Rulemaking |
| RF | Radio Frequency |
| RTCA | Radio Technical Commission for Aeronautics |
| SAE | Society of Automotive Engineers |
| SIF | Selective Identification Facility |
| SMOTEC | Special Missions Operation Test and Evaluation Center |
| STANAG | Standardization Agreement (NATO) |
| TACAN | Tactical Air Navigation |
| TV | Television |
| UHF | Ultra High Frequency |
| U.K. | United Kingdom |
| U.S. | United States |
| VHF | Very High Frequency |
| VLSI | Very Large Scale Integration |
| V/m | Volt/meter |
| VOR | VHF Omnidirectional Range |

Department of Transportation
Federal Aviation Administration

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 15
## ELECTROMECHANICAL ACTUATOR SYSTEMS
## (ELECTRICAL SYSTEMS CERTIFICATION ISSUES)



**PREPARED BY:**

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

**PREPARED FOR:**

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# CHAPTER 15

## ELECTROMECHANICAL ACTUATOR SYSTEMS

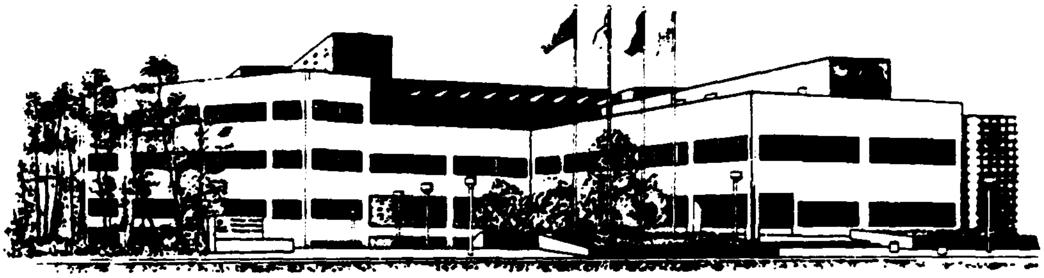
(Not included as of March 1989)

U.S. Department of Transportation
Federal Aviation Administration

DOT/FAA/CT-88/10

# HANDBOOK-VOLUME II
# DIGITAL SYSTEMS VALIDATION

## CHAPTER 16
## ADVANCED VALIDATION ISSUES



**PREPARED BY:**

COMPUTER RESOURCE MANAGEMENT, INC.
950 HERNDON PARKWAY, SUITE 360
HERNDON, VIRGINIA 22070

**PREPARED FOR:**

FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# TABLE OF CONTENTS

TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

# 1. INTRODUCTION

The Aeronautical Policy Review Committee was organized to formulate a plan for the advancement of United States aeronautical capabilities during the coming decades. In 1985 this committee issued a report that established three goals for America's aerospace community. The goals are comprehensive and span all areas of flight-subsonic, supersonic, and transatmospheric. The achievement of these goals will require major technological advances in all aeronautical technologies. Aerodynamic advances will include improved capabilities in computational fluid dynamics and unobtrusive instrumentation. Propulsion advances will include the development of a range of variable cycle engines and hypersonic ramjets. Structural technology advances will include the development of adaptive, thermal, damage tolerant, and propulsion structures. Material technology advances will result in new composites, alloys, and super-alloys being used throughout the aircraft. Flight systems will benefit from faster microelectronics, new processor architectures, and new software technologies. System integration will result in the interfacing of various aircraft systems under a single controlling device.

Two attributes are common to many of the advancing technologies: First, the embedding of intelligent devices into systems; and second, the aggregation of various avionic functions into higher order functions. In this tutorial these attributes will be referred to as Artificial Intelligence (AI) and System Integration, respectively. The intelligent device will virtually always be a digital microprocessor or network of processors, enriched with AI software. The direction of integration is to integrate the flight control function into the propulsion, structural, or aerodynamics system in order that a higher level system be created. The fundamental motives for these changes are decreases in operating cost, increases in service, and increases in safety.

The aforementioned attributes of advancing technology imply that digital avionics systems for coming generations of aircraft will be very different than today's systems. The certification of these new systems will require validation regulations and procedures that are different than those used in the past. This tutorial introduces the issues that will be the basis for the adaptations or changes required in certification procedures. Section 2 of this tutorial is oriented toward advancing technology. Paragraph 2.1 and 2.2 introduce the three national goals and the types of advances anticipated from their achievement. Paragraph 2.3 introduces the rotor and hypersonic aircraft. These are mentioned because they do not fall within the direct purview of the national goals, but will make significant contributions to commercial air service and/or technology. Paragraph 2.4 is an overview of the digital avionics advances anticipated in the future. Research and development efforts in AI and systems integration are highlighted. A generic "smart" engine and a heat removal technique for microchips are discussed as enabling technologies for future digital avionic systems.

Section 3 is oriented to the identification of those technological trends that will require adapting or changing some certification procedures. Paragraph 3.1 presents the Airbus 320, Boeing 7J7, Bell V-22 Osprey, and X-29 as examples of aircraft that may require immediate or near future certification. Paragraph 3.2 presents the propfan propulsion system as an example of an innovation that challenges current validation procedures; Paragraph 3.3 presents the Full Authority Digital Engine Controller (FADEC) and Fly-By-Wire (FBW) technologies in the same vein. Paragraph 3 4 discusses the problems of validating "intelligent" and multi-function systems.

Section 4 contains detailed discussions on a number of issues that are critical to certifying aircraft of the future. These issues include Fiber-Optics, AI, Advanced Controls/Displays, and Remotely Piloted Vehicles (RPV).

## 2. THE DIRECTION OF AMERICA'S AVIATION RESEARCH

### 2.1. Justification

In 1982 a report was issued by a governmental interagency group, under the direction of the White House Office of Science and Technology Policy, analyzing the state of aeronautical research and the role of the Federal Government in supporting that research. The conclusions of that report acknowledged the existence of the potential for advances in aeronautical technology that would result in monumental increases in aircraft performance. It was further recognized that the realization of these advances could only be accomplished by a coordinated effort involving both government and industry. This report resulted in the formation of the Aeronautical Policy Review Committee whose purpose was to track the implementation of the recommendations of that report. In 1985 this committee issued a report (National Aeronautical Research & Development Goals - Technology for America's Future, 1985) that established the specific goals that must be vigorously pursued if the advances are to be realized. This report also recognized that, in addition to the technological problems facing American government and industries, another factor must be considered: competition from abroad. In the interest of national economic and military security, United States aeronautics must meet these challenges and remain a decisive influence in world aviation.

### 2.2. The Goals

The Aeronautical Policy Review Committee established three national goals. When accomplished, these goals will be vital to America's preeminence as a world leader in aviation technology. Efforts on achieving the three goals will proceed in parallel, but with a time-phased order of attainment as depicted in figure 2.2-1 (Lupinetti, 1987). The goals are as follows:

- Subsonics goal: to revitalize aircraft technology.
- Supersonics goal: to attain long-distance efficiency.
- Transatmospherics goal: to secure future options.

The immediate emphasis will be on accomplishing the first goal before the end of the Twentieth Century. This will provide the impetus for continuing the effort and accomplishing latter goals after the year 2000.

### 2.2.1. The Subsonics Goal

The subsonics goal is to move a new generation of subsonic aircraft to a competitive commercial position in the world transportation system. It is important because it is a foundation for latter goals. While United States aircraft still maintain a broad base of technological advantage, the margin

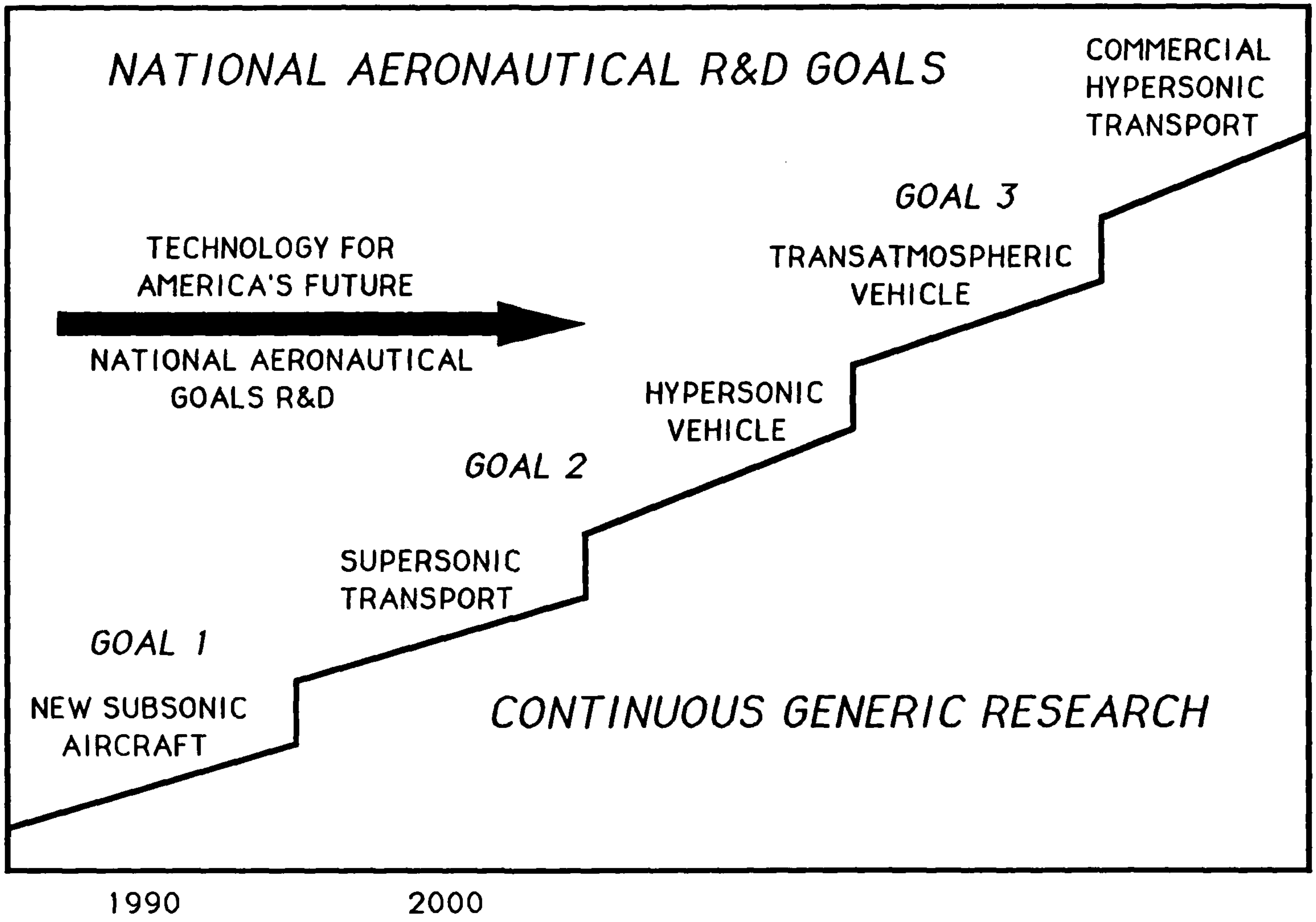

NATIONAL AERONAUTICAL R&D GOALS
COMMERCIAL HYPERSONIC TRANSPORT
GOAL 3
TRANSATMOSPHERIC VEHICLE
TECHNOLOGY FOR AMERICA'S FUTURE
NATIONAL AERONAUTICAL GOALS R&D
HYPERSONIC VEHICLE
GOAL 2
SUPERSONIC TRANSPORT
GOAL 1
NEW SUBSONIC AIRCRAFT
CONTINUOUS GENERIC RESEARCH
1990
2000

FIGURE 2.2-1. NATIONAL AERONAUTICAL RESEARCH & DEVELOPMENT GOALS (Lupinetti, 1987)

of that advantage has been reduced significantly in recent years. In an increasing number of technological areas, foreign capabilities are now equivalent to, or superior to, that of America. During most of the last two decades, improvements in aeronautical technologies have been evolutionary. This will continue, but the new generation of subsonic aircraft must also foster revolutionary technologies. These two approaches to research and development, evolutionary and revolutionary, must produce the resources in the private sector that will enable the exploitation of the ensuing opportunities in supersonic and transatmosperic flight. This goal not only calls for the production of a safe, fuel-efficient, and technically superior aircraft but for a modernized national airspace system. This modernized airspace system is crucial if the benefits from the new aircraft are to be fully realized.

The objective is to have the new subsonic generation of aircraft readied by the mid-1990's. Consequently, the United States would enjoy advanced subsonic technology benefits before the 21st Century. Technologies that are essential to the development of the new subsonic aircraft are as follows:

- Laminar flow control advancements that substantially reduce air drag.
- A new generation of super bypass and propfan engines that will provide a more reliable and efficient operation.
- A new composite, high strain structure.
- More sophisticated, fully integrated flight controls and operating systems that will interface with the new national airspace system.

### 2.2.2. The Supersonic Goal

This goal becomes increasingly important because of changing transportation needs. Strategically and economically, the United States is becoming closely allied with the Pacific community of nations. This is in opposition to past development in the European community. The Pacific region's capacity for growth and development should be encouraged by America's enterprise and policy. A major constraining factor in the developing relationship between the United States and Asia is distance. Supersonic air travel will minimize the impact of distance. The development of technologies required for a new generation of supersonic transport aircraft will provide an opportunity for joint developmental efforts with the Pacific nations. Long-term political bonds may result from these cooperative efforts.

With the elimination of the United States Supersonic Transport effort in 1971, aggressive research and development was curtailed in the supersonic field. However, the Supersonic Cruise Research program, sponsored by NASA, maintained an American presence in this field through 1981; this work provides a basis for continuing the effort. Technological advances in the area of cooling methods, internal aerodynamics, coatings, and single crystal turbine blades offer a means for solving some of the problems present in the original effort. These advancements, when applied to a variable cycle engine with less noise and greater fuel efficiency, offer realistic hope for the development of a supersonic transport.

The report of the Aeronautical Policy Review Committee (National Aeronautical R&D Goals - Technology for America's Future, 1985) credits the following technological advances as being important to the supersonic effort:

- The application of powder metallurgy technology and superplastic forming techniques to load-carrying structures.
- The development of new thermoplastic, carbon-carbon, and metal matrix materials.
- The development of new fault-tolerant computers to assist in load alleviation and dynamic damping.
- The development of supersonic laminar flow that will result in significant reductions in the aircraft weight per pound of payload by providing sustained cruise speeds at much greater fuel efficiency.
- The development of computers with greater computational capabilities that will permit the computation of complex flows and optimizations extending the regions for supersonic laminar flow.

The integration of technological advances into a new supersonic transport aircraft would result in reduction of flight times to five hours or less between the most distant points in the Pacific area. For both commercial and military purposes, this is important to America's future.

### 2.2.3. The Transatmospherics Goal

The United States partitions flight into aeronautics and space. Some of the benefits obtained from subsonic flight can be enhanced in supersonic flight. Some of the benefits of supersonic flight can be enhanced in transatmosperic flight. For the United States to be a decisive influence in the world transportation system, it must have the following capabilities:

- Maneuvering craft into and out of the atmosphere.
- Rapidly responding to needs for low earth orbit missions.
- Attaining very rapid transport services from conventional runways between points on the earth's surface.

These capabilities will be required for America's security, both economically and militarily, in the coming century.

Much of the technology required for the convergence of the aeronautics and space flight concepts will be directly obtained from or will be extensions of the new subsonic and supersonic aircraft. The space shuttle experience will be a major source. In other cases, new technologies will be required. As scarce resources are spent in propulsion, configuration, materials, flight system, and fuel/coolant research, consideration must be given to the unique requirements of the transatmospheric goal.

## 2.3. The High-Speed Rotorcraft and Hypersonic Aircraft

While the three goals of the Aeronautical Policy Review Committee define the direction of aeronautical research and development, it is important to mention two types of aircraft that vaguely fit into these goals: the high-speed rotorcraft and hypersonic aircraft. Table 2.3-1 shows the accepted classes of aircraft by speed range.

TABLE 2.3-1. AIRCRAFT TYPE BY SPEED RANGE

| Type of Aircraft | Speed Range |
|---|---|
| Rotorcraft/Vertical Takeoff and Landing | Hover to Mach Range 0.8 |
| Subsonic | Up to Mach 1 |
| Supersonic | Mach Range 2 to 4 |
| Hypersonic | Mach Range 5 to 12 |
| Transatmospheric | Mach Range 8 to Orbital Velocity |

Strictly speaking, the rotorcraft may be considered subsonic, and the hypersonic may be considered transatmospheric. Because of their unique technologies, they are considered separately in this tutorial.

### 2.3.1. Rotorcraft

The short-haul commuter market is expected to grow extensively in the coming years. Vertical Takeoff and Landing (VTOL) craft, e.g., the tilt-rotorcraft should supply much of the capability for this market. These vehicles should permit commercial travel between center-cities at speeds in excess of present-day helicopters. The tilt-rotorcraft concept came into existence during World War II. When the prop-rotors are facing upward, the tilt-rotorcraft hovers like a helicopter; when they face forward, a turboprop airplane is created that can travel at speeds up to 300 miles per hour. The X-wing aircraft is another rotorcraft design that may service this same market. The X-wing is a stoppable rotor aircraft: when the rotor is active, the aircraft can hover like a helicopter; when the rotor is stopped, the aircraft becomes a conventional aircraft with cruise speeds in excess of 400 miles per hour.

The technology required for these two designs is at hand. Propulsion is by turboprop or turbo-jet; aluminum is the material used for body construction; and conventional hydrocarbon fuels/coolants are used. The major disadvantage is the greater cost per payload-mile, and this may require improvement. However, the convenience of beginning and ending flights at small, convenient heliports, rather than at large airports, offsets this cost to a degree. If this commercial market develops, the certification engineer will be required to create new or adapt existing rotocraft airworthiness rules.

### 2.3.2. Hypersonic Aircraft

This discussion is included for completeness. Hypersonic flight fills the gap between supersonic flight and transatmospheric flight. As noted in table 2.3-1, this spans Mach ranges 5 through 12. The potential commercial applications for transports of this class would be for transoceanic, transcontinental travel, the same as supersonic flight. The major difference is that a Los Angeles International (LAX) to Tokyo flight is estimated to require about 5 hours in a supersonic craft (Mach 2-3) or 2 hours in a hypersonic craft (Mach 5). Supersonic aircraft require conventional airports, while hypersonic aircraft would require extended runways at conventional airports.

Research in hypersonic flight started with the X-15 research program and is currently conducted by the Defense Advanced Research Projects Agency (DARPA). The current long-range cruise missile may be the first operational hypersonic vehicle. The problems of sustained hypersonic flight are significant propulsion and aerodynamic heating. The propulsion system must be able to sustain the Mach 5 and up speeds. The cruise missile uses the supersonic-combustion ramjet (scramjet) burning high-density hydrocarbon fuels. The materials required for hypersonic flight must be able to sustain temperatures of 5000 degrees Fahrenheit. Airframe research using supercold hydrogen is solving this problem. Civil aviation is unlikely to benefit from hypersonic flight or transatmospheric flight until well into the 21st Century.

## 2.4. Advances in Avionics-Related Technologies

Digital avionics is one of the fastest growing technologies in aerospace science. It continues to proliferate throughout aircraft and spacecraft, and finds application in subsystems, such as sensors, system controls, crew function automating equipment, displays, and communications. Research and development is currently underway for commercial FBW and Fly-By-Light (FBL) controls. The Airbus A320 is the first airliner in the world with computer-driven FBW controls which prevent the aircraft from stalling and exceeding speed/acceleration limits. While highly innovative, the Airbus Industrie plane appears already to be a commercial success: 439 booked orders and options from 15 airlines before its first scheduled flight. Certification and first entry service are planned for 1992.

### 2.4.1. Overview of Digital Avionics Technology Advances - Artificial Intelligence

Artificial Intelligence and expert systems are emerging in numerous digital avionics areas. Systems incorporating this technology are being designed to perform the following tasks:

- Coordinating sensor data to determine best flight path, thus avoiding terrain threats.
- Automatically initiating the execution of certain emergency procedures.
- Automatically reconfiguring aircraft systems to optimize performance or correct faults.

Artificial Intelligence and expert systems are software entities, and their emergence in digital avionics is accompanied by greater shipboard computer processing and data storage facilities.

The DARPA and United States Air Force (USAF) are cooperating in the Pilot's Associate program. While this program is directed toward combat pilots, the acceptance of this technology will most likely result in its adaptation for commercial flight. This program's emphasis is on providing the pilot with information and aids for assisting in immediate decision-making; a secondary emphasis is to assist the pilot in longer-range planning. The computer software required for this is a set of cooperating expert systems that operate at very high processing speeds; Lockheed-Georgia and McDonnell Douglas are developing this software. A new parallel-processor computer architecture is being developed to support these expert systems.

Other AI efforts involve the integration of various sensor data into a single composite display. Examples of the sensors being integrated are as follows: ground-mapping radar, stored digital map, and the location of nearby aircraft. AI is also an element in speech recognition. In this capacity, AI has advanced to the stage where a system can learn to recognize a pilots voice in two sessions of less then 60 minutes' duration. This system makes use of the latest ITT (consultant committees for) International Telegraphy and telephony algorithms.

As mentioned earlier, the incorporation of expert systems and AI in avionic systems requires a new approach to software systems development. This is due to the greater logical complexity and the size of the software. Numerous efforts are underway with the objective of streamlining software development and maintenance in this environment; the Air Force Modular Avionic System Architecture is an example. Expert systems and AI will be covered in detail in section 4 of this tutorial. They also apply to other technological improvements, such as Advanced Controls and Displays, Voice Command Processing, Systems Integration, and Robotics. These areas will also be discussed in later sections of this tutorial.

### 2.4.2. Overview of Digital Avionics Technology Advances - Standardization and Integration

In addition to AI, standardization and integration of avionic modules is being emphasized. At this time, the impetus for this effort has been felt primarily in military avionics. In 1986, Congress requested that the services "prepare a joint plan for the inclusion of fully integrated, digital avionics...on all aircraft under development." DOD's (Department of Defense) response to this was the development of the Joint Integrated Avionics Plan for New Aircraft. As a result of this plan, common line replaceable modules will use Very-High-Speed Integrated Circuits (VHSIC). The common line replaceable modules would then be used to build standardized data processors, integrated systems (communications, identification, navigation), and signal processors. Standards for architecture, high-speed data bus, avionics computer, packaging, connectors, backplances, and reusable software modules are in the process of being developed. The Navy Advanced Tactical Aircraft, the Air Force Advanced Tactical Fighter (ATF), and the Army Light Helicopter Experimental are among the initial craft destined for standardization. The effects of standardization and integration will be present in future commercial digital avionic systems.

As FBW and FBL controlled aircraft system designs gain greater attention, the development of digital Cathode Ray Tube (CRT) cockpit displays/controllers and integrated air/ground communication systems increase in importance. The V-22 Osprey, a tilt-rotorcraft with potential commercial usage, has its digital avionic systems highly integrated with other aircraft systems. All information to the pilot is provided through an operator's console consisting of four six-inch color displays. Such parameters as engine speed, engine torque, fuel quantity, fuel rate of flow, and electrical system configuration are displayed through this console. Alphanumeric keyboards with small CRT monitors are used to control the aircraft. The FBW Digital Flight Control System (DFCS) consists of three digital processors, each controlling a MIL-STD-1553 data bus. A digital system uses optical disk for the storage of maps which are used as a supplement to other navigational displays. The detection of faults and subsequent isolation of affected avionics subsystems is performed by digital software. The reliability of these digital systems is resulting in their growing acceptance into the area of flight-critical processing.

Commercial aviation is converging on an integration of air, ground, and satellite digital data links. To facilitate this, agreements are being reached on communications architecture and interface standards. With these agreements, different communications equipment will be capable of sharing data without modification to either equipment or software. An important benefit of this will be the ability to bypass faulted areas of the communications network by the process of rerouting. To some degree, the planned Federal Aviation Administration (FAA) Traffic Alert and Collision Avoidance System (TCAS) will require this technology. To a greater degree, the FAA's Automated Enroute Air Traffic Control System (AERA) will require it. AERA involves a complex modernization of all FAA on-the-ground air traffic computers. TCAS is scheduled to be operational in the near future; AERA is scheduled to begin implementation in the mid 1990's and continue implementation through the early years of the next century.

### 2.4.3. Overview of Digital Avionics Technology Advances - Others

In addition to the areas of AI, standardization, and integration, near-term changes are underway in other avionics-related technologies. Examples of these technological concerns and developments are as follows:

- In converting from analog to digital systems, concern is being directed to safety during the transition period. International activity is growing in the area of increasing Radio Frequency (RF) susceptibility standards and determining field strengths in the geographical areas adjacent to airports.

- Computer architectures are changing to permit greater processing speed and data handling capacity. AT&T has developed a family of signal processors that execute mathematical operations only when data is available, not at fixed time intervals. The advantages to architectures similar to this are rapid allocation of resources, high throughput, and parallel processing of multiple sets of data.

- Computer architectures based on the MIL-STD-1750A processor are being developed. These are being put on a single chip with VHSIC and Gallium Arsenide (GaAs) technologies. GaAs is also being used for cascadable arithmetic logic units, used in embedded computers requiring flexible word-lengths.

- Fiber optics technology is being developed to provide the bandwidth necessary for new digital data buses. Older MIL-STD-1553 buses are being replaced with fiber optic systems with compatible protocols and software. An experimental FBL system is being tested on a Sikorsky JUH-10-60A helicopter that utilizes an AT&T fiber optic bus; the bus appears to operate at 1 Million bytes per second (Mbps) to the user, but is actually operating at 20 Mbps.

- The Boeing 7J7, a next generation commercial aircraft, was tested with a voice recognition system. Twenty-five potential flight deck applications for voice recognition have been identified.

- Analog-oriented functions have been replaced with digital-oriented functions. This replacement has resulted in a reconsideration of the boundaries of hardware, firmware, and software. This has primarily been felt in the digital areas of process controllers with limited branches, single chips, and bit slices. Line replaceable units, earlier considered to be pure hardware, now have embedded processors which require software or firmware. DOD is attempting to standardize new software development around DOD-STD-2167 and modifications to MIL-STD-480.

- Signal processors are now being developed to process two and more functions.

- Reductions in weight and volume with accompanying increases in accuracy are being achieved with new global positioning systems.

- The "fly-by-glass" trend, the use of CRT's in place of traditional instrumentation has been under constant development. The use of CRT's places different workload patterns on the aircraft crew. Human engineering and user-friendly design factors are being approved before aircraft design is finalized.

### 2.4.4. An Application of Microelectronics - The "Smart" Engine

An example of the research underway that dramatically affects traditional technology is the application of microelectronics to propulsion systems. The research cited in this section was performed by A.H. Epstein, and is summarized in ""Smart" Engine Components: A Micro in Every Blade?" (Epstein, 1986).

Most of today's attention in propulsion technology is directed toward the debate over the resurrection of the old turboprop concept in the guise of the "propfan". However, other research is underway that may have major effects on the aircraft of the future. Aircraft gas turbine engines are virtually open-loop devices. They have remained so for essentially three reasons: First, relatively poor sensor technology and limited onboard computational capability have not justified a controller; second, high reliability has been achieved with simple systems; and third, high performance gains have been realized without the need for control loops. However, advances in microelectronics make possible engine control devices with major computational capacities; the result is that gas-turbine components and subsystems may be moved from open- to closed-loop operation. Mr. Epstein feels this may be desirable for four reasons:

- Current engine designs represent a constrained optimization. Improvements in the performance of components or subsystems, off-design, may not result in improved performance of the design: a high thrust-to-weight ratio conflicts with good performance retention and maintainability. A relaxation of these constraints could improve performance.

- Current design practice is expensive; self-adaptive components may allow less expensive development.

- Through dynamic, subsystem reconfiguration, adaptive components could increase damage tolerance and reliability.

- Current technology may not produce the efficient, multifunction propulsion systems that will be required for advanced aircraft.

In order that "smart" technology be incorporated in a propulsion system, a feedback control mechanism must be present that will permit a component's adaptation to local conditions. This feedback control mechanism will consist of sensors, processors, and actuators.

Applications of "smart" engines may be categorized as near-term versus long-term, low risk versus high risk. Examples of potential applications are as follows:

- Active control of turbine blade tip clearance, based on real-time measurements instead of open-loop scheduling. This is a near-term application that has the development of highly reliable sensors as an enabling technology.

- Active exhaust-nozzle position improvement. The nozzle would be adjusted based on data from the aircraft accelerometers, thus improving vehicle performance. Today's continuously variable nozzles operate with pressure mismatches due to nonideal conditions, schedule problems, atmospheric gradients, and other factors. This is a near-term application which requires the development of variable-exhaust nozzles capable of lasting through many adjustment cycles as an enabling technology.

- Active inlet distortion control. High compressor stall margins (on the order of 10-20 percent) exist in high performance military aircraft because of inlet distortions at high angles of attack. This stall margin could be reduced if the compressor distortion tolerance could be dynamically adjusted. This adjustment could be based on local pressure distribution measurements that result in the activation of individual guide vanes. Enabling technologies consist of actuators and sensors of sufficient bandwidth and reliability, and greater understanding of compressor behavior. This is a longer-term application.

- Active noise abatement is one of many additional potential applications.

Common to virtually every potential application are the requirements for significant technological improvement in actuators, sensors, processors, data transmission, and control system architecture. In order that the requirements for withstanding large forces and for small physical size be met, actuators have traditionally used hydraulics. However, their complexity and maintenance characteristics make it unlikely that large numbers of these devices could be used throughout an engine. Large numbers would be required if the engine were closed-loop in design. Electric actuators are desirable if they can be developed to meet the torque, packaging, and bandwidth requirements. Samarium-cobalt motors and piezoelectric devices offer some promise in meeting these requirements, but each has its shortcomings. (Layers of piezoelectric material, dispersed throughout a structure, have been proposed as actuators capable of supplying distributed forces of relatively high frequencies.)

For the purpose of increasing reliability, a designer may provide additional computing elements in the system, rather than add sensors to the engine. Using a single chip to incorporate signal conditioning, transducer, data reduction, and control may provide the needed signal processing while not affecting reliability significantly. Fiber optics may also offer hope for improvement.

Microelectronics, while the catalyst for developing closed-loop engines, may also be a problem. Control elements dispersed throughout a gas turbine engine will require cooling. Current semiconductor technology is restricted to a modest temperature range. Development of high-temperature semiconductor technology is a partial alternative to a cooling system. (See paragraph 2.4.5 for a discussion of chip cooling.) Conceivably, the processing power currently available through microelectronics may be.insufficient. The computational and control functions needed in adaptive applications may be beyond current technology levels. If this is the case, this technology must also be improved.

Advances in microelectronics are commercially driven. The improvements required for aircraft adaptive engines may not result from this commercial motivation. In this instance, motivation may have to be supplied by the propulsion engine community.

Advanced adaptive applications may require control mechanisms beyond the capabilities of current control system architecture. It may even be necessary to distribute the control function over multiple mechanisms. Other subtechnologies, such as nonlinear control and fault tolerance, as well as adaptive control may be utilized.

Questions arise with the issue of certification. How is an engine that contains components and subsystems that are self-adaptive certified? Does every engine require separate certification? The design, as well as the validation and performance verification techniques of the manufacturer, becomes part of the certification process.

### 2.4.5. An Application of Heat Removal Technology - Microelectronics

A major problem in the growing microelectronic technology is chip cooling. If digital avionic systems are going to provide the capabilities required by advanced aircraft, this problem must be solved. As discussed in paragraph 2.4.4, research in the area of high-temperature semiconductivity offers some promise for improvement. Another approach is the use of micro heat pipes. The research and development efforts mentioned in this section were obtained from an article written by Dr. George Peterson; his article (Peterson, 1987) was a basis for this discussion.

A number of recent developments in heat pipe technology offer hope for alleviating the problem of microchip sensitivity to heat. These developments are as follows:

- Large silicon wafers are being cooled by devices that are one-fourth the size and one-seventh the weight of fins, coolant loops, or cold plates, traditional cooling devices. These new devices are being produced by Radio Corporation of America (RCA).

- Transistors are being cooled by a heat pipe method that reduces junction temperature to 63° C at a power level of 40 W. Hughes Aircraft is the developer of this method.

- Cooling systems have been developed with improved thermal response times and reduced thermal resistance for thyristors. Thyristors are solid-state devices that convert alternating current to direct current.

- Before the year 2000, very small heat pipes should be commercially available in the United States. These pipes should play an important part in the development of Three-Dimensional (3-D) chips.

According to Peterson, a heat pipe is defined and operates as follows:

> "A heat pipe is a passive device typically consisting of a sealed container lined with a wicking material and filled with just enough fluid to fully saturate the wick. It operates on a closed vaporization and condensation cycle. Heat added to the evaporator section of the pipe vaporizes the working fluid. The high temperature and corresponding high pressure in this region cause the vapor to flow to the cooler end of the pipe, where the vapor condenses. Capillary forces in the wicking structure generate a positive pumping pressure that forces the working fluid back to the evaporator end."

The operation of the heat pipe is shown in figure 2.4-1. Heat pipes are superior to the best solid conductors, because the pipe has a much higher effective measure of thermal conductivity; this is due primarily to the transfer of heat by the concept of phase change of the working fluid.

Heat pipes are categorized by size: large, medium, and micro. Large heat pipes are used to remove heat from component housings; medium heat pipes are used as mounts for components; micro heat pipes may be embedded within chips. Large heat pipes may be .3 m or longer; micro heat pipes may be less than 5 cm long, and 1 mm in diameter; medium heat pipes cover the ranges in between.

In avionics, a typical use of large heat pipes would be to reduce the heat in housings for various systems or subsystems. Since the housing may be sealed at the points that the heat pipes penetrate, the housing remains a closed system, free from contamination by harsh environments. Medium heat pipes are used as a substitute for single-phase coolant loops or cold plates. These are commonly used to cool semiconductor devices, integrated circuits, or other components mounted on printed circuit boards. In an avionic system, several medium heat pipes may be arrayed into a substrate with a printed circuit board mounted on the substrate. In addition to cooling the printed circuit, this substrate may serve to reduce a "local hot spot". This will increase the mean time between failures of the circuit board. The three research and development efforts alluded to earlier cooling large silicon wafers, transistors, and thyristors use medium heat pipes.

Micro heat pipes should be commercially available in the 1990's. In a commercial semiconductor chip, all chip elements lie in a plane on top of a conducting material, either silicon or GaAs. The effective gate density of a single chip would be increased if the chip contained multiple planes of chip elements; this would enable element interconnections vertically, as well as horizontally. One of the problems inherent in this architecture is the heat buildup that would result. Micro heat pipes offer a potential solution to this problem. Current heat removal systems function at the 50 W/cm$^2$ level. 3-D chip architectures would require heat removal rates of 200 W/cm$^2$. Embedded micro heat pipes could function in this range. Heat accumulations in avionic systems have the following three components: First, the resistance from semiconductor junction to the device; second, the resistance from the device to the heat sink; and third, the distance from the sink to the ambient. The micro heat pipe reduces the heat buildup in the resistance from the semiconductor junction to the device, the largest of the heat components.

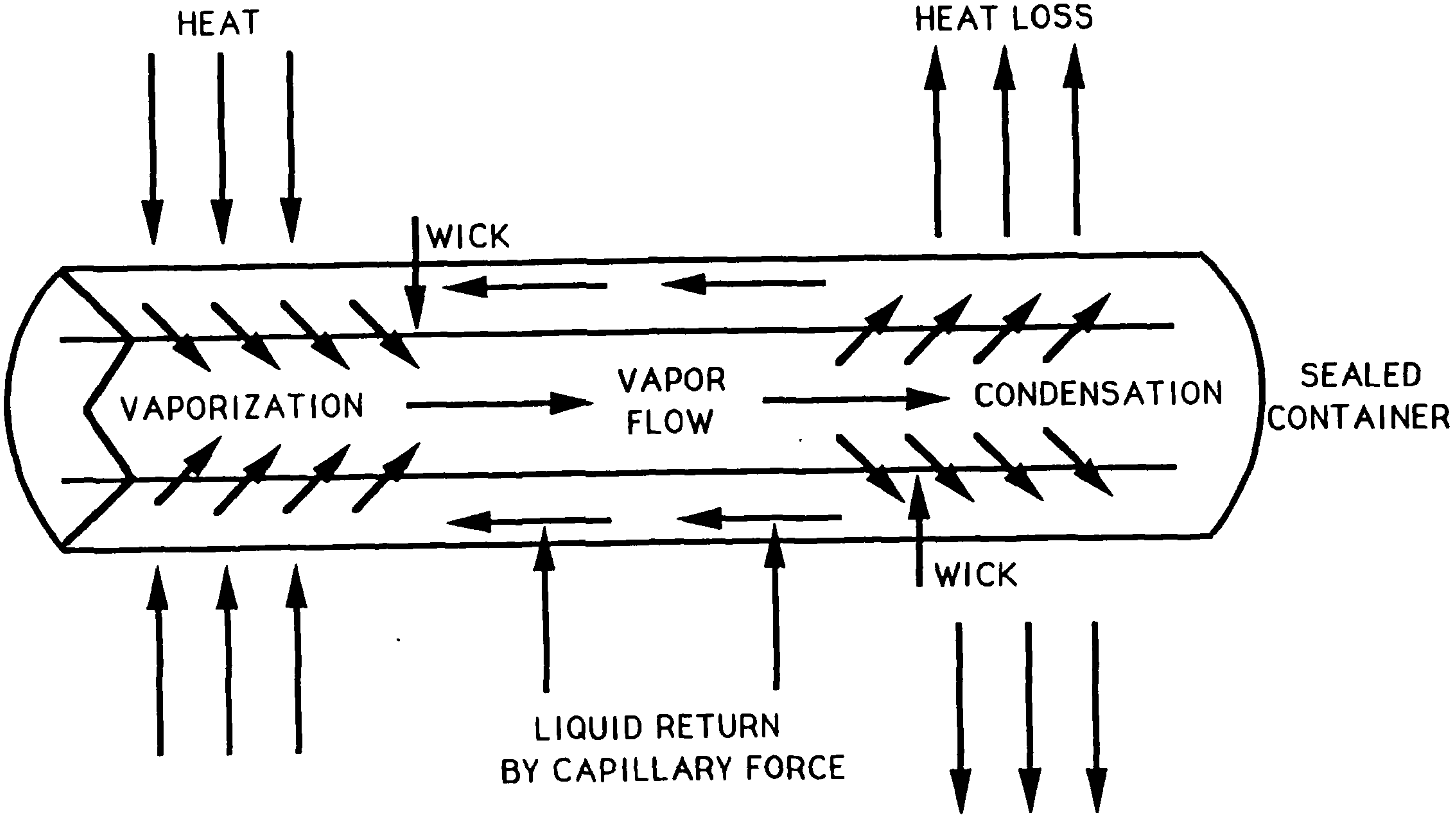


FIGURE 2.4-1. OPERATION OF HEAT PIPE IN MICROCHIP COOLING

One of the enabling technologies for advanced avionic systems, in lieu of the speed, propulsion, and friction anticipated, will be heat removal. Heat pipes are compact and light-weight. If micro heat pipes can become an integral part of 3-D chips, a major advance will have been made.

# 3. CERTIFICATION AND ADVANCING TECHNOLOGY

## 3.1. Challenges for the Certification Process and Regulations

Section 1 discussed the goals that will be driving aerospace technology for several decades. Conjecture was also given on the general technological advances that are required to support the achievement of those goals. The supersonic and transatmospheric aircraft required to meet their respective goals lie somewhat in the future; however, it is reasonably certain that there will be a new generation of commercial subsonic aircraft in use before the year 2000. The new technologies found in these aircraft pose a challenge to traditional certification procedures and regulations.

### 3.1.1. The New Generation of Subsonic Aircraft

Airbus Industrie's entry in the new subsonic generation utilizes today's technology; the assumption being that currently available technology is more than adequate to meet the needs of the airlines over the next decade or more. The Airbus Industrie A320 is a narrow body, short range aircraft; the A330 and A340 are the wide body, long range aircrafts. There are plans in Airbus Industrie to have their new aircraft ready for certification and service by 1992.

The FBW technology incorporated in the A320 will tax certification regulations. With FBW technology, heavy mechanical and hydraulic aircraft systems are being replaced by electronic wiring; the result is an "all-electric" airplane. In any Flight Control System (FCS) using FBW there is a set of sensors which produce electrical inputs into a flight control computer. There are also a number of actuators on the end of the communications link which drive control surfaces. The flight computers take signals from all sensors, cross monitor them, produce consolidated signals, and identify them as the best information. The computers then process the aircraft's control laws, determining what the control surfaces should be doing. Control signals are either forwarded directly to the control surfaces or to actuator drive units.

On the A320, FBW will be used on all surfaces for the rudder and tailplane trimming reversionary mode. Hydraulic activation is used on all surfaces. The FBW system incorporates two elevator aileron computers and four spoiler elevator computers. These computers drive left/right combinations of aileron, ground spoiler/speed brakes, and elevator left/right surface segments. The pitch axis control includes an automatically trimmed horizontal stabilizer. The ailerons and spoilers also receive inputs from a load alleviation system. For pilot control, side-sticks are used in lieu of control columns. The side-stick includes the autopilot disconnect feature, the radio communication/interphone switches, and a datum adjust switch for varying selected headings and vertical speeds.

Boeing plans to introduce its next generation aircraft, currently called the 7J7, by the mid-1990's. It has been announced that the 7J7 will take advantage of emerging technologies in propulsion, aerodynamics, structures, materials, aircraft systems, and cabin design. It will be powered by ultra-high bypass engines.

### 3.1.2. A New Application for Vertical Takeoff and Landing Aircraft

In addition to the new subsonic aircraft, the year 2000 may also see VTOL craft playing a major role in commercial aviation. This craft will most likely utilize either a tilt-rotorcraft or X-wing design. The military success of the Bell XV-15 and its larger version, the V-22 Osprey, give the tilt-rotorcraft design the advantage. Bell has issued a design proposal for the Bell D326 Clipper, a commercial version of the V-22. Numerous turboprop aircraft are now used by "third level" commercial carriers. Such aircraft as DHC-7's (DeHavilland Twin Otters) and Shorts 330's dominate this market. A civilian version of the V-22 would probably carry 44 passengers. The United States Marine Corps version carries 24 fully armed assault troops.

The potential advantages of VTOL craft replacing turboprop craft are significant. As mentioned earlier, travel between cities serviced by third level carriers would be between center-cities, not between major airports. To the traveller, this may mean greater cost since VTOL craft are less fuel efficient; however, the time saving may be great. VTOL travel in this marketplace has been estimated to be three times faster door to door than any other combination of vehicles. When the cost of ground transportation is considered, the cost differential may lessen, or even disappear. To the air travel community as a whole, the reduction in airport and airway congestion may be major; air travel may become considerably safer. Airline deregulation has increased the problem of congestion. Conventional jet aircraft now fly on many of the well travelled routes much more frequently with deregulation. Third level carriers have grown in number to service the routes deserted by the trunk lines; these carriers usually fly lower performance aircraft. The third level carrier aircraft use the same runways as the high performance aircraft flown by the trunk carriers. If the third level carrier used VTOL craft, simple airport facilities could be used that were remote from major airports and convenient to center-cities. An example of this is a feasibility study conducted by the Port Authority of New York and New Jersey on using the Manhattan Battery Park heliport for XV-15 landings and takeoffs.

Another potential market for tilt-rotorcraft is the corporate air travel market. This market is currently serviced by planes such as the Learjet. The advantages to the traveller and the air travel community are similar to those previously mentioned.

### 3.1.3. The Experimental Aircraft - X-29

The new generation commercial subsonic plane(s) and the tilt-rotorcraft are two new aircraft fostering new technologies that will impact certification Another aircraft that is an indicator of even more advanced technological change is the X-29. The A320 incorporated new technology but at a moderate pace. Performance improvements of 5 to 10 percent over existing aircraft may be expected in aerodynamics, structures, propulsion, navigation, communication, and FCS's. The A320 will utilize the CFM56-5 or IAE V2500 turbofan engines. The 7J7 is a bit more radical. The initial use of polymer material in the airframe, a flight management system with stability augmentation, and an ultrabypass engine is estimated to improve performance another 10 percent beyond the latest turbofan aircraft. A generic subsonic aircraft using laminar flow technology and ultra high bypass propfan engines, as well as active stability augmentation and very high aspect ratio supercritical wings, is estimated to improve overall performance by 60 percent over today's aircraft. The X-29 is considered most radical.

The X-29 is an advanced technology experimental aircraft developed under the guidance of the DARPA and the National Aeronautics and Space Administration (NASA). The X-29 incorporates the following new technologies:

- Forward Swept Wing: provides aero efficiency.
- Close Coupled Canard: low-speed control.
- Thin Supercritical Airfoil: control at high angle of attack.
- Discrete Variable Camber: enhanced maneuverability.
- Relaxed Static Stability: favorable volume distribution.
- Three-surface Control: increased agility.
- Aeroelastic Tailoring: solves aero divergence.
- Composite Wing Covers: reduces drag and weight.
- Triplex Digital Design: flexible/multiple modes.
- Fly-By-Wire: tailor handling qualities.

The X-29 possesses an inherent 35 percent negative static stability margin: a design feature enabling extensive maneuvering abilities, yet offering a severe control system problem. The FBW DFCS stabilizes the aircraft, permitting normal, acceptable handling. The control laws for the NASA's Space Shuttle, NASA's F-8, and the Air Force AFTI/F-16 could not stabilize this degree of negative static margin. The pitch instability of the X-29 is four times that of the AFTI/F-16. Therefore, the development of the X-29's control laws and a DFCS capable of stabilizing the aircraft is a major accomplishment.

The DFCS was designed to exploit the aerodynamic advantages of the aircraft, e.g., the forward swept wing and the close coupled canard. The DFCS is multi-mode and has three channels. The system uses seven F-16 National Waterlift actuators to drive the two canards, six segmented-trailing-edge flaperons, and a single rudder. A newly designed actuator drives each of the two strake flaps. Flight control computers, air-data sensors, and an attitude reference system are the remaining components of the DFCS. Each of the three digital computers has an analog backup in parallel. Exercise of the several modes provides a graceful degradation feature when components begin to fail. Normal operations use the full digital mode and the associated automatic camber control. A normal approach mode controls takeoff and landing. There are two reversion modes:

- A digital reversion mode using different software than that used in the normal mode. This mode does not utilize noncritical sensors.

- An analog reversion mode. This mode is only activated when there is a generic digital control fault.

The up and away, power approach, and ground contact for weight on any wheel operational regions are available with each mode. There is also a precision approach control mode which enables the pilot to directly control flight path angle by means of a pitch stick. When switching between modes, precautions have been taken to minimize transients.

While the immediate beneficiary of X-29 technology is the ATF program, it is a matter of time before advanced civil aircraft will likewise reap benefits. A successful experimental aircraft is expected to increase performance by five to ten times that of existing aircraft. Experimental aircraft are being studied jointly by NASA and the Navy for an oblique wing design, and by DARPA and NASA for an X-wing rotorcraft design. The future holds promise for an experimental aerospace plane. The technologies fostered in these experimental craft extend beyond subsonic flight and into supersonic and hypersonic flight.

### 3.1.4. New Aircraft - Summary Comments

The requirement for change is the same whether the certification domain is transport, rotorcraft, or small general aircraft. New systems oriented to today's technological categories will affect changes in certification regulations and procedures. Examples of these are Upper Surface Blowing (USB) propulsive lift and the propfan engine. FAA certification procedures, as of 1984, did not allow for the advantages of powered lift technology as incorporated in USB designs. NASA has found the USB design to be fuel-efficient for low-speed, Short Takeoff and Landing (STOL) flight; current research is testing its performance in high-speed flight. If the technology is adapted to civil use, FAA certification must follow. The propfan propulsion design is a resurrection of the turboprop engine. The propfan, a result of NASA research, incorporates new propeller technology in an energy efficient engine. Paragraph 2.4.4 of this tutorial introduced microelectronics to a propulsion system on a theoretical basis. Most propfan designs utilize microelectronic digital devices for propeller control functions, devices not yet FAA certified for that purpose. The electronic devices will be located in the vicinity of the corrosive exhaust system of the engine, a high temperature environment. While the microelectronics will be used for propeller control, e.g., pitch change control, it will not be used for adaptive control of the engine elements. The propfan is an example of revolutionary engine/propeller design, augmented by digital avionics.

### 3.2. A Specific Problem for Certification - The Propfan

Current air-worthiness regulations do not directly cover the design features present in the latest technological advances. Propfan or ducted/unducted variable pitch fan propulsion system designs are examples. As a response to this, the FAA is taking steps to assure that certification programs will accommodate the latest technologies. "New Propulsion Concepts and FAA Certification" (Aerospace Engineering, 1988) describes the difficulties in certifying the propfan.

The intention of the Federal Acquisition Regulation (FAR) is to classify aeronautical products into types and to define the minimum requirements for certification. Each product type is covered by a unique regulation called a Part. The product type is evaluated against its respective regulation. As examples, Part 25 contains the criteria against which transport category aircraft are evaluated; Part 33 contains the criteria for aircraft engines; and Part 35 covers aircraft propellers. In the past, engines and propellers with the propfan design have been classified as two distinct product types. This classification must be reconsidered for accuracy. FARs permit the stipulation of special conditions when the existing regulation does not seem to cover the particular product type. The intention of the FAR is to promote public safety, not define limitations of aircraft design. Special conditions are required for the propfan. These conditions must guarantee that the aircraft containing the propfan propulsion system achieves the safety standards demanded by Part 25, while the propfan satisfies the standards established in Parts 33 and 35.

One of the problems with propfan certification is the requirement for containment of the propeller blade. Part 33, the engine regulation, stipulates that any failed or released fan blade must be contained within the engine housing. This requirement is based on traditional turbofan engine design. In a turboprop-based design, the blades are not shrouded and do not have any means of containment. With safety as the underlying motive, it is then necessary to provide the design measure that minimizes the chance that a blade will fail or be released. Part 25, the transport aircraft regulation, stipulates that the aircraft must be able to withstand the impact of a failed or released blade with no structural damage that would pose a hazard to the safety of the aircraft. Applicants for certification must demonstrate that the aircraft can sustain the structural damage caused by a failed or released blade, and that the aircrafts other critical systems will continue to operate correctly during the period of blade loss. The propfan applicant should demonstrate that in his aircraft the probability of blade loss is acceptably low, and that the structure of his aircraft is such that blade loss would not jeopardize the safe continuance of the flight.

A second problem is that the propeller hub found in a propfan design may differ significantly from that found in traditional propeller aircraft. The differences are in the areas of size, number of blades mounted, and temperature environment. Propfan propeller hubs are large, have several blades mounted, and operate in a high temperature environment. Blade retention strength is the prime safety consideration for the propfan hubs; the FAA requirement is that the hub's blade retention strength be sufficient to ensure that the loss of a blade is a virtual impossibility. If the hub is part of the turbine rotor, then its shattering may be a greater threat to the structure of the aircraft than blade loss. Adequate margin between load and material strength should be a design attribute to eliminate this safety concern. All propfan components, the hub included, must demonstrate that they do not deteriorate measurably when exposed to the exhaust stream of the engine (high temperature vulnerability). To summarize, the propeller hub (blade retention facility) cannot be sufficiently validated by the precise criteria contained in Part 35. The criteria must be supplemented with special conditions to show that the same safety objective is achieved.

A third problem is the propfan pitch control system. It is a digital electronic control system. Digital avionics have now been incorporated into the propulsion system. Digital electronic control devices have not yet been certified by the FAA for propeller control. The pitch control mechanism for the propfan also includes mechanical or hydraulic linkages and a two-stage counterrotating rotor. All of these are not traditionally found in the pitch control system. The safety goals are as follows:

- No failures that result in excessive propeller speeds that may result in fragmentation.

- No failures that will result in a high drag condition.

- No control system failure that results in an undesirable command to autofeather (automatically move the propeller to zero drag position).

Current industry design practices have resulted in pitch control mechanisms that satisfy these safety requirements. The problem of certification is to assure that the corresponding propfan mechanism demonstrates the same degree of airworthiness.

A fourth problem is the design of the propfan propeller blade. These blades may be more susceptible to time and usage than traditional blades. Propfan blades are characterized by swept platforms, wide chords, and thin airfoils. They are made of layers of composite material, enclosing a light filler material. As such, they may be more vulnerable to chemicals, foreign object damage, heat, and humidity. Because of this, it will be necessary to track each blade and hub to determine its performance history. Periodic inspections for durability, flutter, vibration, and stress will also be required. This is not required for normal propeller blades and hubs. These are usually certified for an unlimited life, given that certain maintenance levels are sustained. As a result, detailed records of time-in-service are not maintained. Another safety concern over the propfan blade is that composite material does not conduct electricity as well as metal; therefore, the effect of lightning strikes must be determined.

Other potential problems with propfan certification lie in the areas of potential gearbox failure due to the high horsepower ratings, noise, and safety requirements for aft-fuselage mounted engines. As examples of the latter, minimum clearance standards are different for aircraft with engines mounted behind the fuselage and ingestion of foreign objects is of greater concern when propellers are located at the rear of the craft.

The propfan is an example of a product of a growing technology that has novel and unusual design features. These design features are not addressed in current certification regulations. However, the issuance of and compliance with special conditions will assure that proper controls are in place for assuring public safety.

### 3.3. A Specific Problem for Certification - The Rotorcraft

Certification rules for helicopters have evolved as helicopter technology has advanced. As avionic systems utilizing microprocessor technology are increasingly used in helicopters, these certification procedures will be challenged. There is a major concern with respect to the impact of digital electronic controls on civil helicopters. Technologies such as mechanical systems, pneumatic systems, and hydraulic systems are mature and are covered by the "specific rules", of air-worthiness regulations which state specific requirements. As electromagnetic and electromechanical technologies were increasingly used in helicopter systems, certification procedures migrated from specific rules to "general rules". With a general rule, more emphasis is placed on achieving a desired safety level and less on how that safety level is achieved. One of the purposes in doing this was to maintain safety standards, but not constrain design. Some of the difficulities of certifying helicopters using advanced technologies are described in "Certification Issues in Civil Helicopters" (Brahney, 1988). The information contained in this section is based on "Certification Issues in Civil Helicopters" (Brahney, 1988) and information obtained from John D. Swihart, Jr., and Richard Vaughn of the FAA.

#### 3.3.1. The Full Authority Digital Engine Controller

The FADEC was one of the first systems introduced in a helicopter that utilized advanced control technology. The FADEC uses microelectronic technology instead of the traditional hydromechanical technology; the former offers increased accuracy, improved control modes, better maintenance, and substantially reduced life cycle costs. The FADEC must operate in a hostile environment for thousands of hours without failure or maintenance. The components of the FADEC use leadless chip carriers and include advanced 16-bit microprocessors with error correcting memory, analog/digital converters, pressure/thermal sensor signal converters, and digital data bus interfaces. The Sikorsky S76B is equipped with the FADEC.

There are two general rules in FAA regulations that are applicable to the certification of helicopters which use systems based on advanced control technologies. FAR 29.1301 covers the operation of the systems in the aircraft; FAR 29.1309 specifies the interaction between the system and the helicopter environment, and the acceptable ramifications of system failures. Software validation for the FADEC requires demonstrating through testing in the helicopter environment that the system is not only logically correct but that the user's requirements are satisfied. Errors may exist that result from software deviations from requirements and from timing considerations during program execution. The software must be evaluated by testing that begins with a sequence of stand alone tests, proceeds through simulated engine tests, continues with testing on an engine test stand, and culminates with flight test. A difficulty with software testing is that general rules in certification require that the testing procedures and results be verified. This means that the FAA must review documented test results, as well as software development documentation. In the absence of a standard, this documentation will be unique to each manufacturer. Until recently, there was no movement for development of standards for software documentation.

3.3.2. Fly-By-Wire Technology

The incorporation of microprocessor technology in helicopter FCS's is more recent than its use in power plants. This innovation has come in the form of FBW. The V-22 Osprey tilt-rotorcraft is an example of a tilt-rotorcraft that utilizes FBW technology. Since FCS's are more relevant to flight safety than FADEC, this innovation is viewed differently by the FAA. In FBW technology, flight safety will be almost completely in the hands of microprocessor controls. The certification of these FBW subsystems for safety is of critical importance. The specific and general rules that are applicable to these subsystems must be sufficient for assuring public safety. There are three major concerns in this area:

- The reliability of the electrical power supply system.

- The security of the FBW subsystems against electromagnetic hazards.

- The reliability of embedded software.

While these concerns are mentioned in the context of certifying FBW technology in rotorcraft, they are equally applicable to certifying FBW in fixed wing aircraft, e.g., Airbus A320.

3.3.2.1. Electrical Power System Reliability

With the introduction of digital electronic control systems in FCS's, the importance of the electrical power supply systems has been elevated. Since the FBW subsystems are critical to flight safety, the electrical power systems supplying energy to them must always operate at a level sufficient for sustaining the FBW subsystems' functioning. Consequently, the validation and certification of these electrical power systems is of major importance to the FAA. The power systems must be tested thoroughly under both normal conditions and conditions in which system errors occur.

3.3.2.2. Security Against Electromagnetic Hazards

Prior to FBW, a helicopter's avionic systems did not perform flight-critical functions. Usually the avionic systems controlled only instrumentation not essential for the safe landing of the helicopter. In this situation, electromagnetic hazards were of little concern. With the proliferation of microprocessors throughout flight-critical systems, this is no longer the case. Since High-Energy RF (HERF) fields (generated by commercial radio broadcast transmissions and radar installations) and lightning strikes occur with some frequency, their effect on critical electronic rotorcraft subsystems must be considered. For the purpose of certification, although there are some similarities in the protection against HERF fields and lightning strikes, the major differences to be considered include:

- Amperage: Amperage from RF fields is in the milli- to microampere range while amperage from lightning strikes is in the kiloampere range.

- Frequency: Frequencies from HERF are mainly greater than one megahertz. Frequencies from lightning are mainly less than one megahertz.

- Interaction: Lightning attaches directly to the aircraft in isolated spots. A HERF field envelopes the entire aircraft.

- Effects: A major difference in effects is that lightning can cause burnout or destruction while HERF can only upset or cause glitches in systems.

Because of the use of electronic devices in flight-critical subsystems, the FAA is issuing voluntary testing standards for certifying that the electronics of an aircraft are adequately shielded against electromagnetic hazards. The need is acute because not only are flight-critical subsystems becoming more susceptible to electromagnetic hazards, but protective metal airframe skins are being replaced by nonconductive composites. Since graphite composites are not good conductors, they cannot shield interior circuits. Currents resulting from high-energy fields now move directly along interior conductors. Advances in circuitry also aggravate the problem for the following reasons:

- Increases in microcircuit bandwidths result in increases in the bandwidth against which they must be protected.

- Miniaturization of circuitry decreases the operating voltage which increases the amount of protection required.

Protection from HERF fields can be achieved by either shielding the desired component or subsystem with a conducting material or by isolating the component or subsystem electrically from induced charges. A combination of the two methods may be most desirable for reasons of weight and cost.

The FAA standards initially only covered structural damage to aircraft; but the latest standards, modeled after those developed by the Society of Automotive Engineers (SAE), are more comprehensive. These standards are documented in the SAE Committee Report (SAE Committee AE4L Report No. AE4L-87-3). They were the basis for early approvals of FADEC systems. An aircraft meeting the new standards is expected to be able to withstand lightning strikes with currents in the 200 kiloamp (kA) range. These strikes usually occur only once every few hundred aircraft-years of flying, but the standards should be adapted to protect aircraft from the maximum currents and maximum rates of rise of lightning.

While the FAA standards may be in place, the avionics technology required to meet them will not be easily achieved.

### 3.3.2.3. Embedded Software Reliability

The standard accepted by the FAA for certifying software in flight-critical systems is Radio Technical Commission for Aeronautics (RTCA) document DO-178A. However, this document states that the procedures contained therein are not sufficient for assuring an acceptable level of safety for flight-critical systems. The FAA has recommended that manufacturers providing systems with embedded software conform to DO-178A. Exceptions have been made when redundant software is present. In this instance, the FAA has stipulated that:

- There must be at least two different software systems.
- There may be no shared software modules.
- Each software system must be capable of performing all critical functions independently of another software system.

### 3.3.2.4. A Backup for FBW - Fluidic Flight Control

Some of the concerns expressed in paragraphs 3.3.2.1 and 3.3.2.2 would be alleviated if there were redundancy to the FBW system. Test results from experimentation with a fluidic FCS serving as backup to FBW is discussed in "Fluidic Flight Control: Early Test Results" (Aerospace Engineering, 1988).

In hostile environments, such as high temperature, vibration, and Electromagnetic Interference (EMI), fluidic flight control is being considered as a functionally redundant, nonelectric backup alternative for FBW. The motivation behind this research is the failure probability that exists in FBW systems that is non-existent in traditional hydromechanical FCS's. The composite FCS is a full authority, two-axis, lateral-directional control system for a Navy T-2C aircraft; the tests are being conducted at the Naval Air Development Center.

The selection of either FBW or the fluidic flight control modes is under pilot control. There are no transients when the modes are switched because the idle system is always in active standby status. Early test results indicate that using fluidic technology as a backup for FBW in aircraft subject to high temperature buildups, vibration, and EMI is a viable alternative.

### 3.4. The General Problem for Certification

In paragraph 3.2 the propfan propulsion system design was criticized from the certification point-of-view. In paragraph 3.3, the difficulty of certifying new rotorcraft because of its use of recent advances in microprocessor technology was detailed. In this section, difficulties of a broader nature will be discussed.

### 3.4.1. Intelligent Components, Subsystems, and Systems

Intelligent components, subsystems, and systems that are applied to many systems involving microprocessor elements are emerging as individual technologies. Their emergence as technologies has paralleled the technological growth made in digital computers and storage devices on the microelectronic level.

### 3.4.1.1. Adaptive Components and Subsystems

Adaptive components and subsystems are intelligent components that are characterized by digital controls containing logic that adapts to meet the needs of different inputs or environments. These adaptive components and subsystems create problems for type certification. Questions arise including:

- How are requirements defined?

- How is a system containing one or more self-adapting subsystems type certified?

- Does each system require independent certification?

These questions must be answered if certification regulations and procedures are to accommodate advancing technology.

The cost of fuel is a major factor in acceptance of an aircraft design. For this reason, such measures as seat-statute-miles-per-gallon have gained acceptance as figures of merit for judging propulsion system design. Figure 3.4-1 (Lupinetti, 1987) demonstrates an estimated tripling in performance between the introduction of the first generation turbofan engines through the anticipated propfan engine. One element in the current trend is to gain further engine performance improvement through "smart engines". At this point, digital avionics impacts propulsion systems. Paragraph 2.4.4 of this tutorial discusses a "smart" engine in detail. Aircraft gas turbine engines have historically consisted of an integrated set of open-loop subsystems with a feedback fuel control. Only a few sensors are used to provide inputs, through a feedback process, to a simplified engine model; the controller is based on this model. Restricted onboard computing capacity, insufficient sensor reliability, and insufficient sensor adaptability to harsh environments have dictated this simple control scheme. Advances and anticipated advances in microcomputer technology remove much of this restriction. It has been proven that the use of real-time intelligence (available today with the processing power of microprocessors and data stores) in closed-loop control can be used to improve performance and operability of propulsion system components and subsystems. Propulsion system components and subsystems include, but are not limited to, inlets, fans, compressors, turbines, and nozzles. The theory is that advances in onboard processing capability and sensor technology will enable the incorporation of feedback control within engine components, thus optimizing engine performance and life expectancy.

At this time, research activities are underway identifying the ways to use real-time intelligence for improving propulsion system controls. The specific areas expected to benefit from this identification are compressor stall alleviation, active clearance control, secondary airflow modulation, and active pattern factor control based on blade stresses and temperatures. The enabling technologies involve improving sensor systems, computer systems, effectuator systems, and component models. The continuing revolution in microelectronics suggests that control over factors determining fuel consumption will continue to grow. Among the technological elements of this control are adaptive control, nonlinear models, model fidelity, and fault tolerance. This improvement should alter fundamentally the nature of gas turbine components and subsystems from an open-loop to a closed-loop operation, resulting in optimal performance.

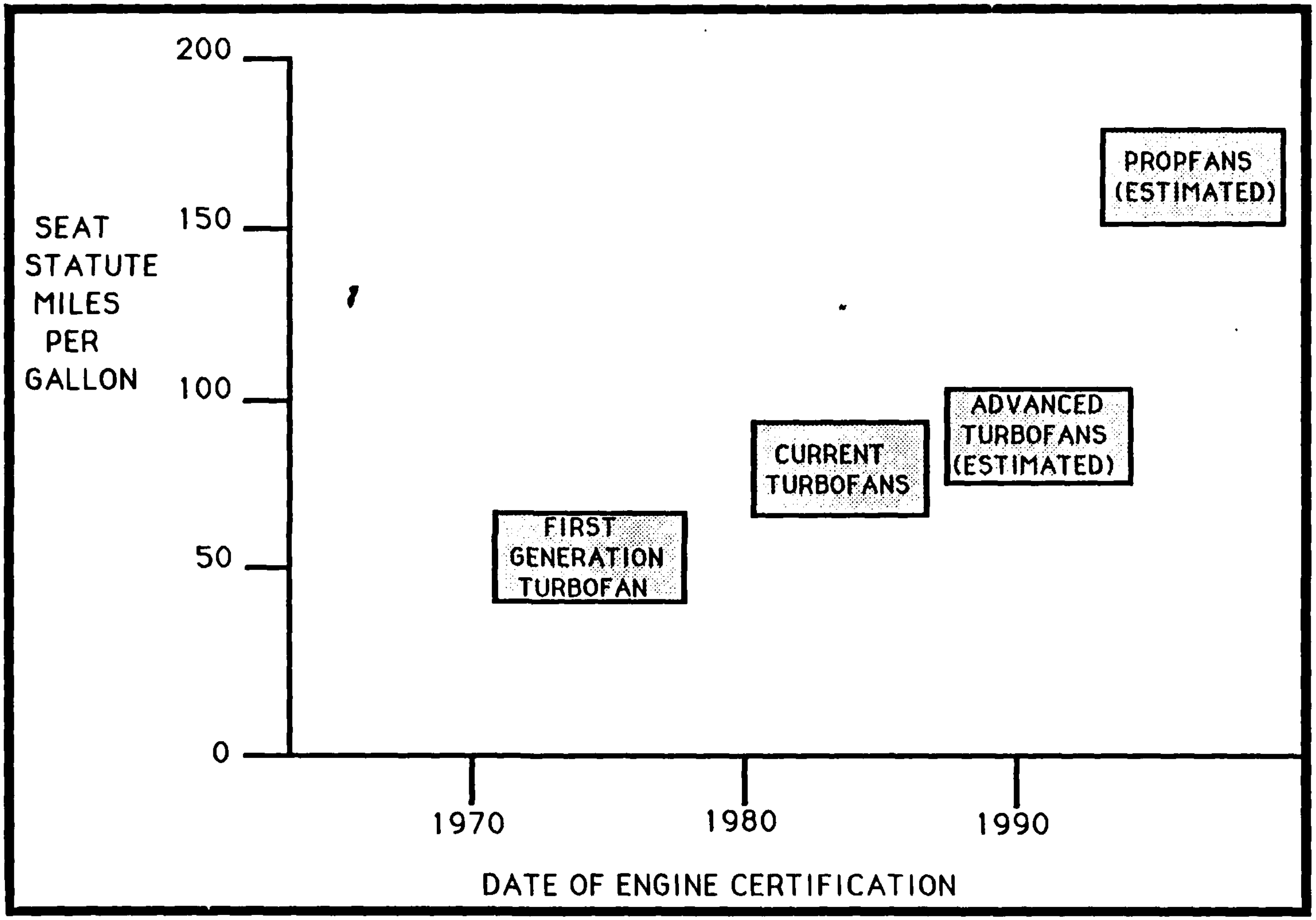


FIGURE 3.4-1. AIRCRAFT PERFORMANCE BY PROPULSION SYSTEM (Lupinetti, 1987)

### 3.4.1.2. Artificial Intelligence and Expert Systems

Artificial Intelligence and expert systems were introduced in paragraph 2.4.1 as being an elemental discipline for emerging avionic technologies. AI is a branch of computer science that creates "intelligent" computer systems that understand, learn, reason, and solve problems. Expert systems are systems that use knowledge and construct inferences regarding problems that would otherwise require human expertise; expert systems result from an application of AI. Rapid advances in AI have only been possible because of the increases in computing power and data manipulation enabled by today's digital processors and data stores. Information processing technology has been advancing approximately by a factor of ten every five years; this pace has been maintained for the past thirty-five years. The problem posed for certification of a digital avionic system utilizing AI is similar to that discussed in paragraph 3.4.1.1; the system does not conform to a rigid set of specifications. Its response to a given stimulus is dynamically determined and time dependent. At a different point in the learning process, the system may respond to the same set of stimuli differently than before. Adaptive control, as discussed in paragraph 3.4.4.1. may incorporate learning, but is more likely not to. For this reason AI-based systems' certification rationale must be based more on a demonstration of the manufacturer's design and the integrity of the manufacturer's performance verification techniques, than on conformance to rigid specifications.

Artificial Intelligence, while having been an academic subject for many years, is still in its infancy. The technology for implementing quasi-intelligent subsystems should be in place by the year 2000. At this time it should be mature enough to support its application in aeronautical system products and processes. An expert system is an example of a quasi-intelligent system. Using a set of facts and rules, the expert system is able to reason. Figure 3.4-2 is a schematic depicting the structure of an expert system. Facts represent inputs to a situation interpreter and actor, the "inference engine". The set of facts is referred to as a "situation base". The inference engine also processes rules from a "knowledge base". The result of processing the facts against the rules is an action or conclusion. Facts are inputs derived from particular sensing mechanisms. Rules are complex data structures that define what relationship of inputs (facts) leads to a certain conclusion (action). The inference engine is an interpretive computer program that applies inputs to rules, and initiates an action when a rule is satisfied.

The major difficulty with expert systems is the need for complete specification. In the design of a large system, a designer must provide a complete definition of all permissible states together with a number of state transition diagrams which specify all transitions between states. An expert system uses a complete set of rules that explain how to find all permissible states, and how to determine which transitions are permissible between states. An expert system requires that all knowledge on a system's functioning be gathered and encoded into a knowledge base. The operation of the system is modified by changing the rules that constitute this knowledge base.

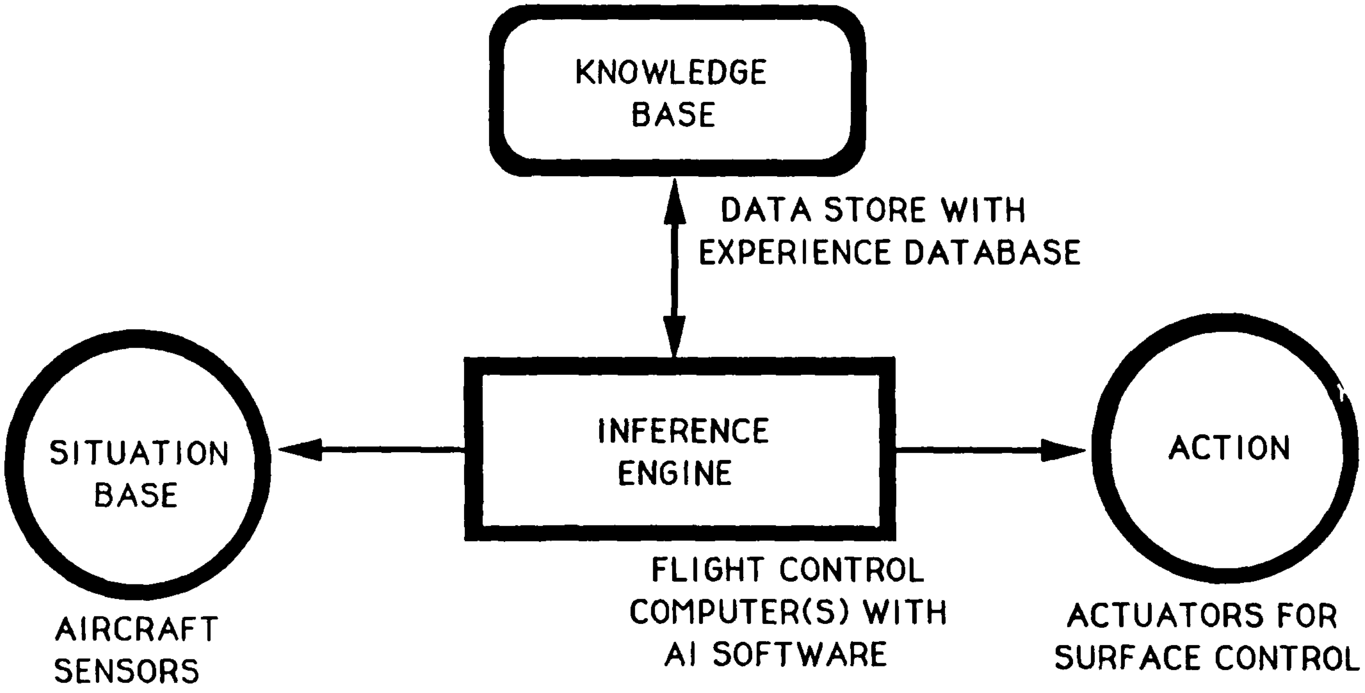

KNOWLEDGE BASE
DATA STORE WITH EXPERIENCE DATABASE
SITUATION BASE
AIRCRAFT SENSORS
INFERENCE ENGINE
FLIGHT CONTROL COMPUTER(S) WITH AI SOFTWARE
ACTION
ACTUATORS FOR SURFACE CONTROL

FIGURE 3.4-2. EXPERT SYSTEM

Improvements in this technology are not tied to the inference engine, but to the acquisition and organization of knowledge in the domains that are relevant to the system. The manual acquisition organization and the structuring of the knowledge base are the major bottlenecks in this process. A knowledge base of 1000 rules may require many man-years of effort to develop. By the year 2000 it is anticipated that there will be specialized expert subsystems in common use that will utilize knowledge bases containing several thousand rules. These subsystems will be limited in scope and applied within a distributed, multifunctional airborne environment. While a limited number of such systems exist today, they are restricted to non-time-critical applications. By the year 2000, expert systems with moderately sized knowledge bases will be used in real-time applications.

As with any system, an expert system is only capable of accomplishing what its designer plans. When we say a system "learns", we mean a knowledge base is improved. The difficulty of translating a discipline into a knowledge base is not to be underestimated. In doing this, structure and quantification are being applied to subjects unaccustomed to it. Frequently, these subjects behave in the planned manner for reasons other than those anticipated by the designer.

In addition to expert systems, AI is also an elemental discipline for Theorem Provers, Robotics, Goal Seeking Systems, Vision, Speech Recognition, and Natural Language Understanding. These are expected to result in new technologies that will be beneficial to the aeronautics community.

### 3.4.2. System Integration

System Integration was introduced in paragraph 2.4.2 as being an elemental discipline for emerging avionics technology. Traditionally, avionic systems have consisted of a collection of individual components, each performing a function independent of other aircraft systems. With the advent of powerful microprocessors, avionic system designers were able to fully integrate navigation, display, and control systems. Integration implies sharing of the data produced by several different sensors and computers. This sharing has the cooperative effect of improving the quality of decisions that can be made by either human or electronic intelligence. When Automatic Control Systems (ACS) are used to stabilize the aircraft, conventional aerodynamic stability requirements can be relaxed. Modern tactical aircraft have low, and even negative, levels of longitudinal static stability; thus, maneuvering capability and cruise performance are enhanced. It is only possible to fly an aircraft with this level of longitudinal static stability because of a full-time, full-authority automatic stability augmentation system that stabilizes the aircraft. Integration also implies the physical consolidation of system functions, which offers its own advantages.

Guidance, Navigation, and Control (GNC) systems will be a forcing function in aircraft design during the coming decades. With today's microprocessors, the designer can exploit the interaction and integration of aerodynamic, structural, and propulsion system controls to provide better, more efficient aircraft.

The advantages of integrated design have been demonstrated in experimental aircraft. The following are two examples:

- Integrated digital control of engine inlet and autopilot systems have resulted in a significant range increase.

- Integration of wing extensions with an active control system have resulted in significant cruise performance improvements.

These are considered to be first generation improvements resulting from system integration. More significant improvements should be realized by the year 2000. The Aeronautical Policy Review Committee (Review of National Aeronautics Policy) states that:

> "Systems integration will play an increasingly important, if not dominant role in the development of advanced technology aircraft... advances in the traditional aeronautical disciplines will no longer ensure a superior product."

While hardware advances in the next two decades will provide greater computational capability, improved reliability, and reduced component cost, these will not be the pacing technology developments. The application of a multidisciplinary design approach to these developments is the challenge of research and development.

The following is an example of the demands that will be placed on a tactical aerospace vehicle by the year 2010 (Aeronautics Technology Possibilities for 2000: Report of a Workshop, 1984).

> "... it will have to deal with massive amounts of information such as: targets, ground and airborne threats, navigation data, route options, weather, weapons, aircraft system status, and commands. This information will have to be collected, stored, processed, correlated, integrated, analyzed, and acted upon in a very short period of time."

The aircraft computer systems must be integrated to accurately process this magnitude of data. Equivalent integration requirements will exist for civil aircraft.

### 3.4.2.1. Current Efforts in System Integration

As mentioned earlier, system integration is now at the first generation level. Intermediate level integration involves the linking of selected functions or subsystems for the purpose of achieving improved performance and has been accomplished. An example of this is the coupling of the throttle, flight control, and navigation systems to provide automatic flight path control. Figure 3.4-3 depicts the state-of-the-art schematic for system integration above the intermediate level. The five circles represent the five major disciplinary areas of aeronautics. The intersections represent functions that have been integrated as a result of a design decision. The solid circles within intersections represent those integrated functions that have been accomplished in production or research aircraft.

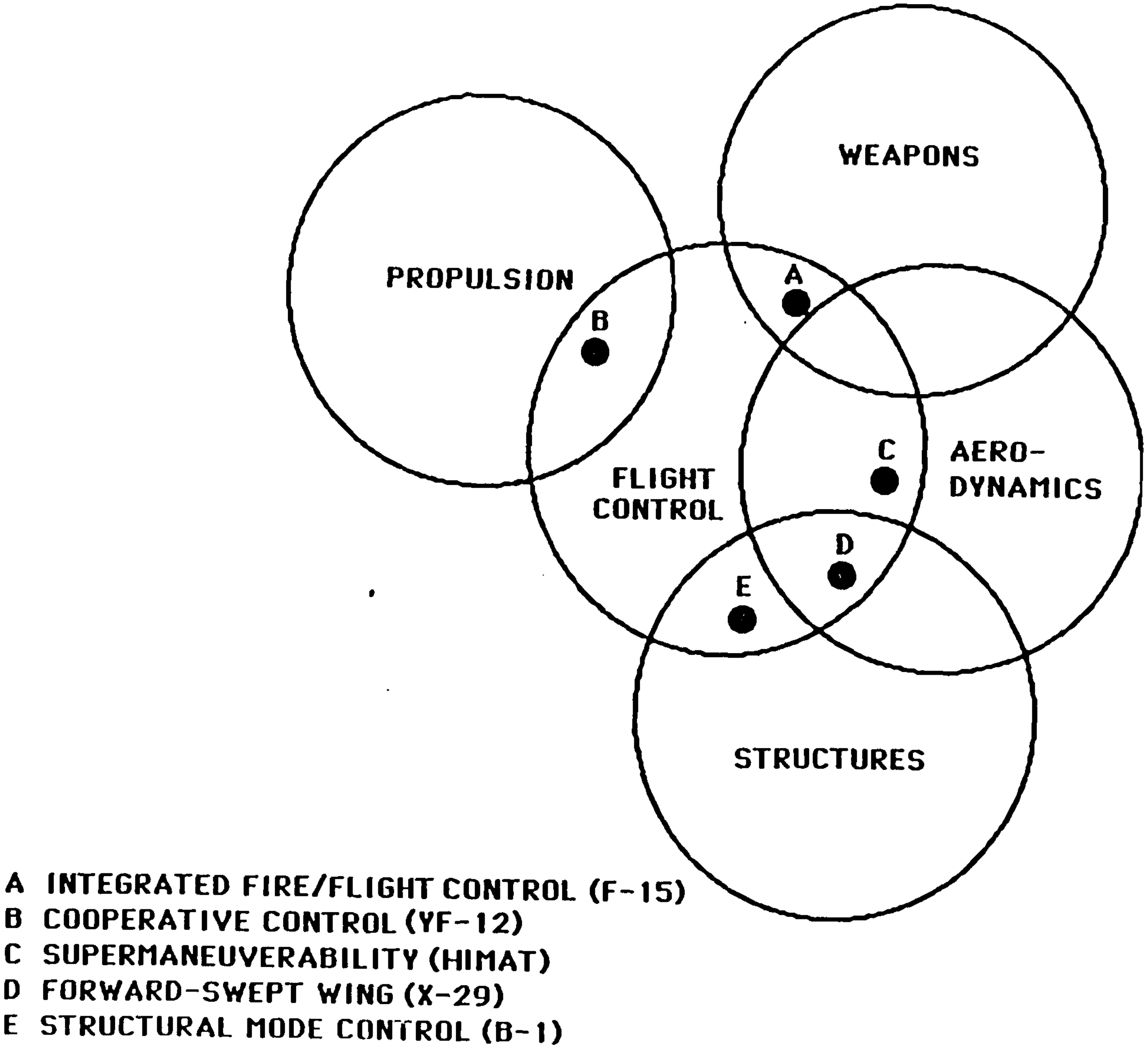

WEAPONS
PROPULSION
A
B
FLIGHT CONTROL
C
AERO-DYNAMICS
D
E
STRUCTURES
A INTEGRATED FIRE/FLIGHT CONTROL (F-15)
B COOPERATIVE CONTROL (YF-12)
C SUPERMANEUVERABILITY (HIMAT)
D FORWARD-SWEPT WING (X-29)
E STRUCTURAL MODE CONTROL (B-1)

FIGURE 3.4-3. SYSTEMS INTEGRATION

The potential advantages of these integration efforts are enormous. The following results are expected:

- An integrated GNC will permit engineers to trade inherent stability for weight and drag reductions.

- An integrated control and structural system will permit engineers to design structures to achieve minimum weight by load control at key points, maximizing load factor capability over the complete dynamic range of the aircraft.

An example of technological advance for the purpose of enabling system integration is the Advanced Fuel Management (AFM) program. This program is under Navy sponsorship; its purpose is to improve aircraft performance by a full integration of the propulsion control and FCS's. A thorough discussion of this program is given in "Moving Closer to Fully integrated Control" (Brahney, 1986). Engine control technology must be improved to make this system integration possible. The unit that controls the propulsion system must be as reliable as the FCS's. The design guidelines ensure that the control unit continues to operate the engine, without performance degradation, following the failure of any single mechanical or electrical component. Selective redundancy was included on the control unit to achieve reliability. The inclusion of selective redundancy in the control unit was the method by which reliability was to be achieved.

The decision to use selective redundancy as a means of achieving desired reliability levels eliminated "single string" electronics architecture as a possible approach to control unit design. The FADEC and Full Authority Fault Tolerant Electronic Engine Control (FAFTEEC) established that dual redundant system architecture is a viable approach to providing high reliability in controlled propulsion systems. However, neither of these designs was adequate for tactical aircraft of the 21st century. For this reason the AFM program was initiated. According to the design specification, the AFM system must integrate fuel, hydraulic, electrical, and mechanical components into a dual channel, full authority, fault tolerant, engine control system. It is responsible for monitoring engine status, reading appropriate data, and scheduling selected parameters for the purpose of achieving a desired engine performance level. Power Level Angle (PLA), certain speeds, temperatures, and pressures are the primary inputs. The outputs are scheduled parameters that relate to engine efficiency, e.g., gas generation and augmenter fuel flow parameters. Figure 3.4-4 is a schematic of the AFM.

The AFM system is composed of three subsystems: the fuel subsystem, the airflow subsystem, and the electronics subsystem. The major components of the fuel subsystem are flow sensors, fuel pumps, and valving. This subsystem is responsible for pumping and metering the fuel to the gas generator and augmenter. The major components of the airflow subsystem are vane and nozzle actuators. This subsystem is responsible for controlling the variables that affect engine airflow. The major components of the electronics subsystem are engine harnesses, generators, and controllers. This subsystem monitors the fuel and airflow subsystems. Figure 3.4-5 demonstrates how the AFM system interfaces with the FCS and the propulsion system (engine).

### 3.4.2.2. Barriers to Implementing System Integration

Experience with integration efforts, like the AFM, shows that the most significant barrier to integrated control is the difficulty of incorporating integrated systems in aircraft. Incorporating systems is difficult and very risky due to the uncertainty of the performance of the aerodynamic, structural, propulsion, and environmental systems under normal and failed flight conditions. Additional problems to be considered are implementing safety precautions to ensure reliable and safe operation and operating without concise measures for rating performance levels.

Current technology is not designed to facilitate system integration. There is emphasis on the Input-Output concept of system operation. The system is not designed to process all the different combinations of inputs and outputs, and there is not enough understanding about how the different technologies interface. Systems engineering is attempting to solve this interface problem, but is handicapped by the absence of higher-level design tools, accurate model definitions, and experience in applying tools in real-world situations..

Some specific design needs are as follows:

- Development of measurements for successful/unsuccessful flight systems performance in aircraft that incorporate state-of-the-art technology, in particular, high-authority DFCS.

- Development of design methodology and techniques for designing in an environment of distributed, parallel processor architectures.

- Development of system architectures that provide high degrees of reliability and dynamic reconfigurations for flight-crucial systems. There is a supporting need for the development of test and assessment aids for ensuring that systems developed satisfy the requirements.

- Development of practical optimization algorithms to accurately extract data from large databases. This processing will be in near real-time mode to assist the pilot in flight path prediction and flight decision making. Distributed and parallel computer architectures, and supporting software may be required.

- Development of software validation and verification methods that are less subjective than the methods currently in use and that maximize existing automation technology.

- Development of techniques for task allocation among crew and vehicle systems based on mission requirements and human error theory.

- Development of models for use in multidisciplinary design for highly interactive systems. Specific examples are as follows:

    - Dynamic response of aeroelastically tailored structures.

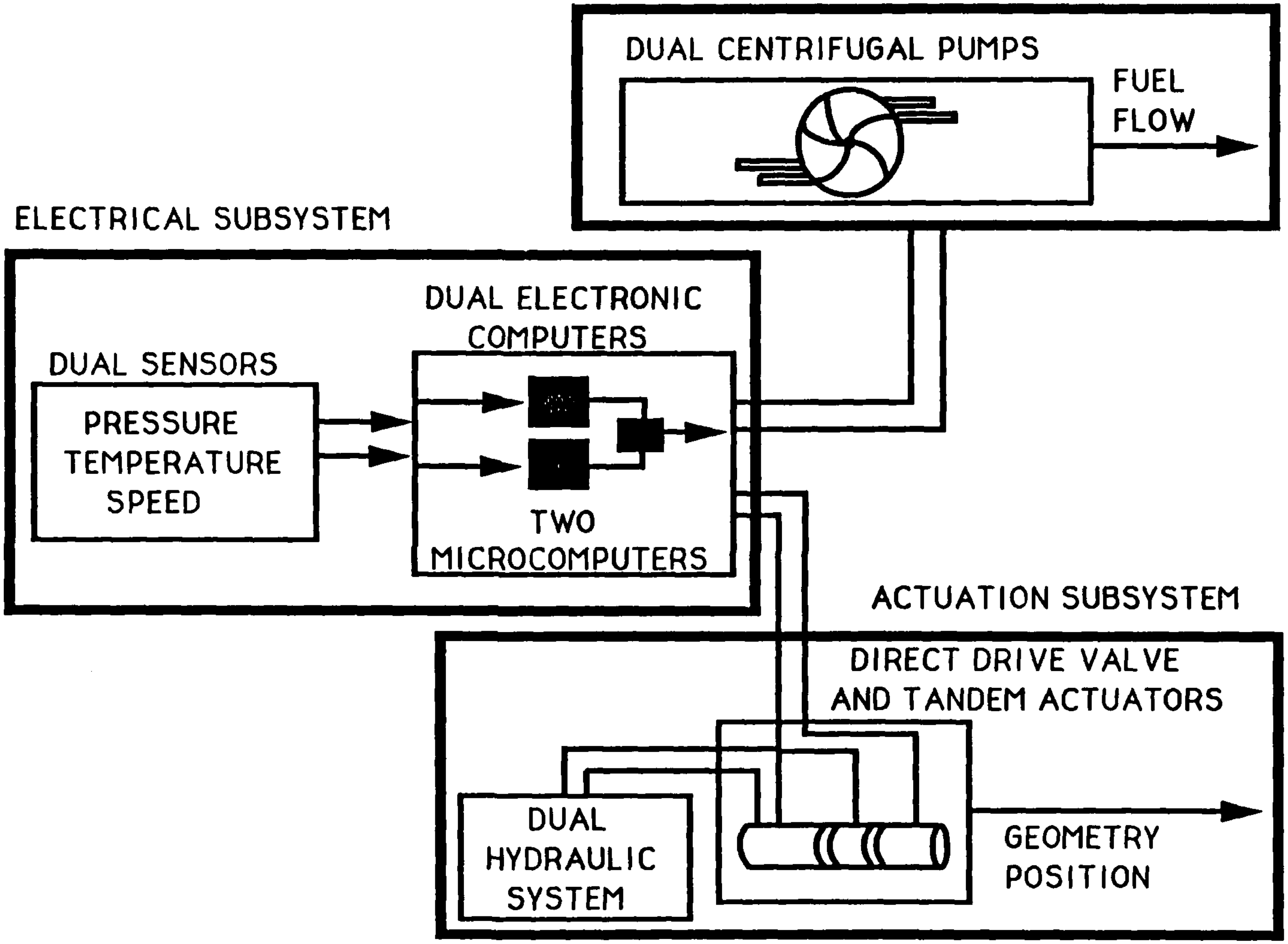


FIGURE 3.4-4. ADVANCED FUEL MANAGEMENT SYSTEM (TOTALLY REDUNDANT)

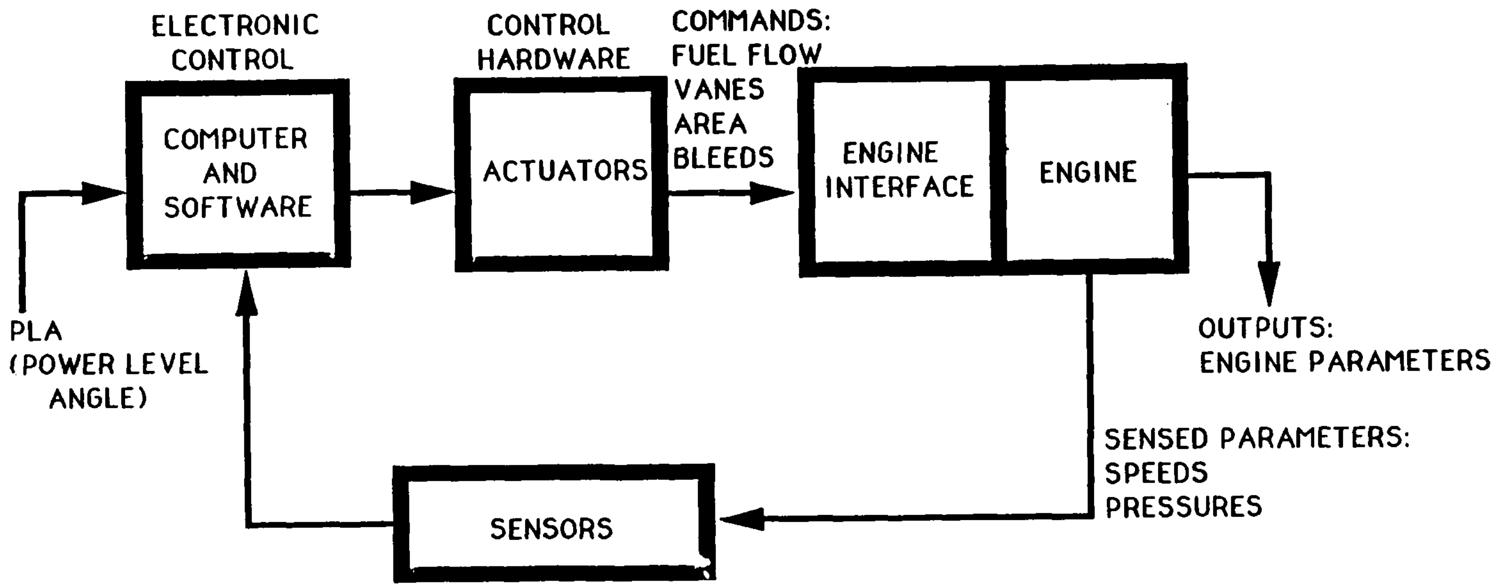


FIGURE 3.4-5. ADVANCED FUEL MANAGEMENT SYSTEM INTERFACES

- Unsteady dynamics at high angle of attack.

- Interaction of engine, inlets, and nozzles.

- Pilot-command/external-disturbance environment for advanced aircraft with state-of-the-art systems.

- Development of computer-assisted design techniques for efficient multi-input and multi-output control for a large number of control parameters. (Practical optimization algorithms for simplifying complex feedback mechanisms are also required.)

- Development of better hardware simulation methodology for building simulator interfaces that permit a more realistic test situation.

### 3.4.2.3. Advantages to be Gained from System Integration

System integration at the highest level will not be achieved without the development of efficient design and analysis tools. The GNC system will be the impetus for aircraft design integration. The key technology will be the multidisciplinary design of interactive aircraft systems that will meet both civil and military performance requirements for speed, range, maneuverability, navigation, efficiency, and safety. In the case of military aircraft, observability and threat avoidance will also be important. Inherent in this methodology will be the ability to resolve serious design conflicts across supporting technologies. When these multidisciplinary designs are fact, the following benefits are possible:

- Reductions in weight and drag by permitting compensation for unstable aerodynamic, structural, and propulsion conditions using a highly authoritative GNC system. Such factors as maneuver load control, gust load alleviation, active flutter suppression, and relaxed static stability would be involved.

- Providing new mission capability (e.g., low observability or super-maneuverability) by permitting compensation for unstable aerodynamic, structural, and propulsion conditions using a highly authoritative GNC system.

- Increasing capabilities for maneuvering, trimming, and STOL by integrating highly interactive subsystems such as vectored thrust and aerodynamic control.

- Maximizing capacity for military aircraft to conduct complex attack/defense missions by integrating fire, flight, and propulsion system controls.

Aircraft development will benefit from a reduction of costly, time-consuming iterations resulting from adverse interactions between systems and unrealized performance goals. Resultant aircraft systems should require less redesign and refinement over the life of the aircraft. These systems should result in less risk, cost, and time for developing new aircraft.

The multidisciplinary design is viewed as an enabling technology for advanced combat aircraft (fighters, multimission rotorcraft, and VTOL), advanced supersonic transports, hypersonic aircraft, and transatmospheric aircraft. The multidisciplinary design will result in improvements in subsonic aircraft.

# 4. RELATED VALIDATION ISSUES

## 4.1. Fiber Optic Technology

Fiber optics is a branch of optics concerned with the propagation of light along thin fibers. Each fiber consists of a core and sheath; the core and sheath are different transparent materials. In practice, more than 100,000 fibers that are a few microns in diameter have been grouped in a single bundle. Light entering one end of a fiber is transmitted the length of the fiber by internal reflections.

Ground-based telephone and data transmission systems, using twisted-pair and coaxial cable technologies, are now being replaced with fiber optic systems. The primary advantages of the fiber optic technology are the greater band-width (approximately 1,000 times higher), and smaller size.' The application of fiber optics to aeronautics offers the advantages of lower cable weight, less space required by conduits, and less vulnerability to the nearness of power cables. In aircraft using composite structures, instead of traditional metallic, the advantage is even greater: less vulnerability to high-level RF interference from power cables, lightning, and other electromagnetic noise.

### 4.1.1. Fly-By-Light

Fly-By-Light is an outgrowth of FBW. In an FBW system, FCCs receive inputs in the form of electronic signals from numerous sources: sensors, avionic systems, pilot control, and maintenance input. In the case of pilot control or maintenance inputs, the FCC may initiate an adjustment to a control surface directly. The control laws for the aircraft exist as a portion of the software for the FCC. Normally, sensor and avionic system inputs are processed through the control law software, and a decision is made that some control surface adjustment is required. The FCC will then send an electronic signal to a control surface or to an actuator controlling a control surface resulting in an adjustment. Usually, heavily shielded coaxial cable is used for the data communications between the FCC, its input sources, and its output destinations. In an FBL system, an optical data bus or bundles of light-sensitive fibers would replace the coaxial cable. Figure 4.1-1 is a schematic of a typical FBL system.

Figure 4.1-1 is a simplified schematic of a system utilizing a single multi-processor control computer with a single channel. In reality there would be multiple systems and channels configured in a redundant architecture. The Primary Control System (PCS) consists of pilot controls, a processor, and actuators. The processor has an electrical power source. The communication between the processor and the pilot controls, and the processor and the actuators is by optical fiber bundles. The PCS is a flight-critical system

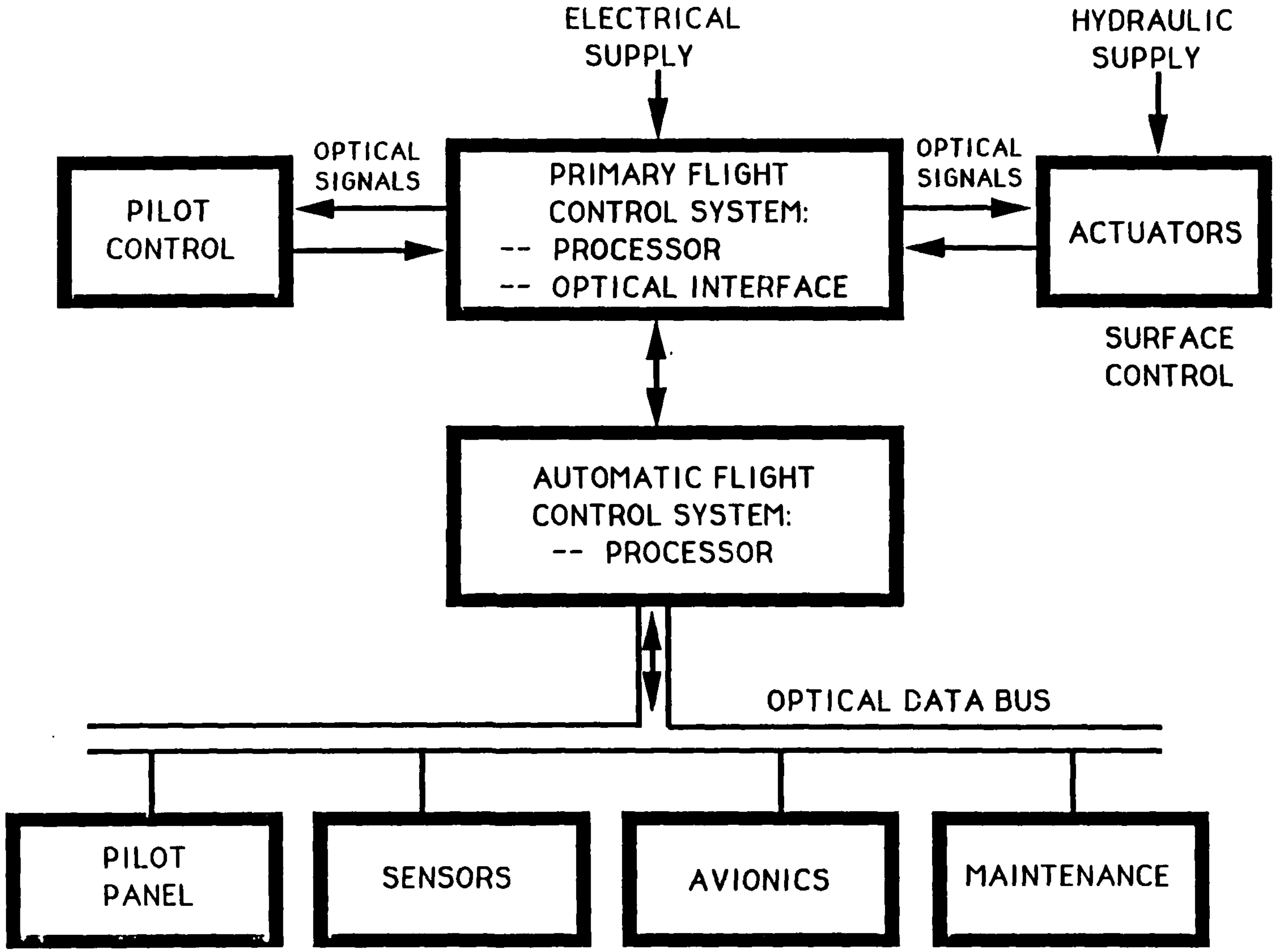


FIGURE 4.1-1. FLY-BY-LIGHT SCHEMATIC

and would therefore be heavily redundant. Flight safety reliability is required of the PCS. The actuators drive control surfaces, so they would most likely require a hydraulic supply.

The ACS consists of a processor, optical data bus, and the following interfacing systems: sensors, other avionic systems, pilot malfunction, and maintenance. The criticality of this system varies. If the aircraft has a high pilot workload or has a high degree of inherent instability, this system may be quite critical. If it is critical, it would involve a high degree of fault tolerance and redundancy. The ACS receives all necessary sensor data through an optical interface with the mission equipment bus in highly augmented/automated/integrated craft. The ACS software is mission-oriented and performs such functions as control law processing and selection of automatic modes. The ACS processor does not communicate with control surface actuators but accomplishes that purpose through the PCS processor.

A major function in a system similar to that defined in figure 4.1-1 is the conversion between optical, electrical, and hydraulic energy forms. An Electronic Interface Unit (EIU) would most likely be used to (1) interface with the processor through a Transistor-Transistor Logic (TTL) compatible buffer, (2) house a transmitter that performs electrical-to-optical conversions, (3) house a receiver that performs optical-to-electrical conversions, and (4) display diagnostic data. A fiber interconnect cable would connect the EIU to a transducer. A digital optical rotary position transducer may be used for pilot input. A digital optical linear position transducer may be used for actuator feedback. Digital optical differential hydraulic pressure transducers may be used to feedback differential pressure between cylinders of a hydraulic actuator or to prevent the force flight between cylinders with different pressures. Controlling an actuator with an optical command may require the conversion of the incoming command to an electrical signal; this signal may then control a conventional electrohydraulic servovalve. A solution to this problem may involve a hydraulic-oriented conversion or a photoelectric conversion. The photoelectric conversion, while seeming obvious, would probably require too much input power. A hydraulic-oriented conversion is probably most practical. This approach does not introduce the need for a new energy form since hydraulic power is already available in the actuator. A turbine-driven alternator or a piezoelectric crystal stack using hydraulic pressure for pulsing the stack ends are state-of-the-art approaches to this conversion.

### 4.1.2. Fiber Optic Sensors

Figure 4.1-2 is an application of fiber optic technology to a wing structure. This wing may contain a large number of sensors that would be subgrouped. Each subgroup would contain a number of binary coded sensors such as code plates, switches, and shaft speed sensors. The sensors of each subgroup would be multiplexed via a singlemode optical fiber to an optical receiver. The receiver would be a component of an EIU which would convert the binary encoded data to an electronic signal and buffer the data to a processor.

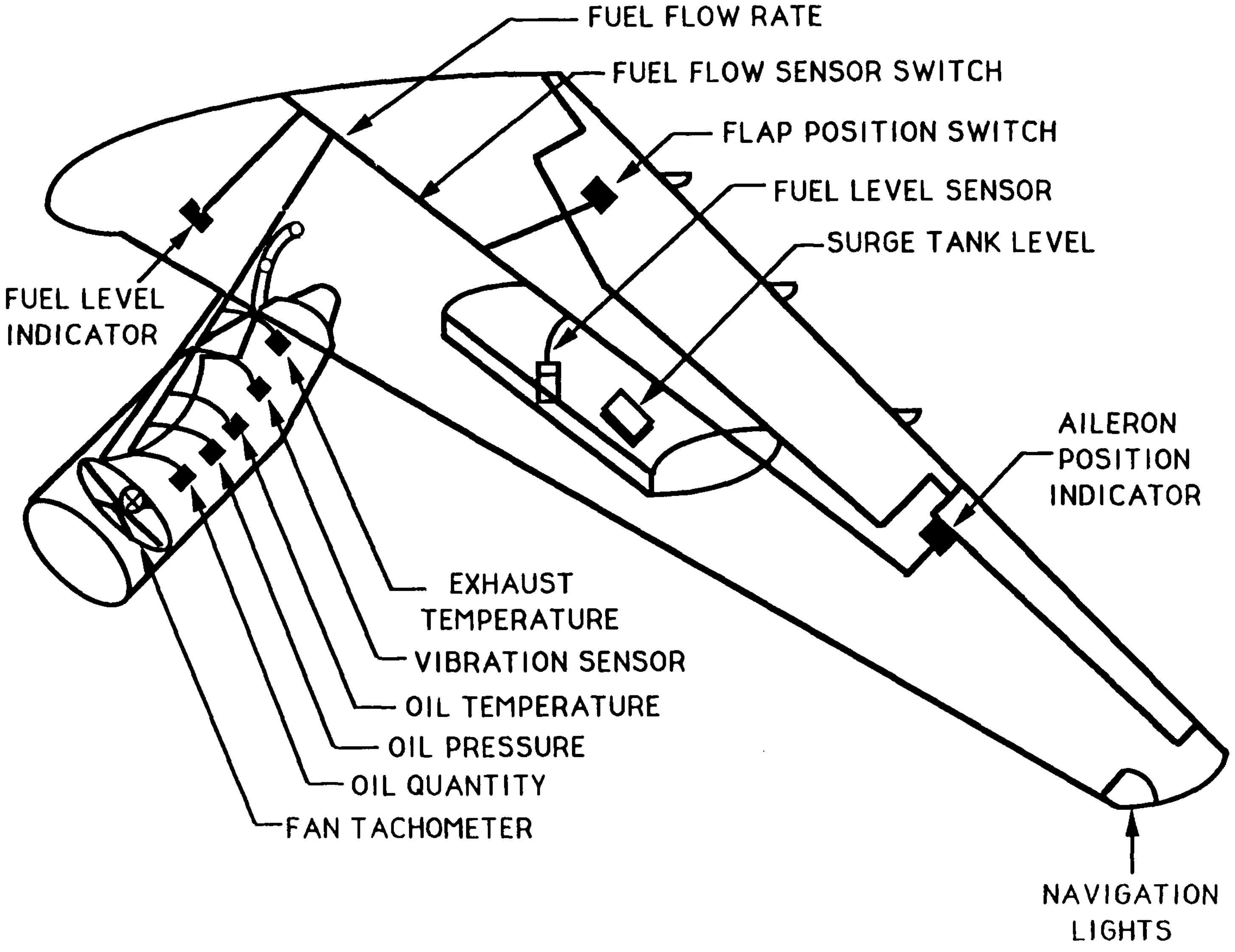


FIGURE 4.1-2 FIBER OPTICS IN WING ASSEMBLY

Due to the relatively large size of fiber optic connectors and the large number of sensors, it is necessary to multiplex data gathered from several sensors over a single fiber. A transducer using multimode fiber optic delay lines with a pulsed laser diode is frequently used as a multiplexor. This multiplexing scheme represents a traditional time division multiplex system. An advantage of this system is the use of a serial binary readout. Disadvantages are the system data losses and delay intervals inherent in time based multiplexing. Research on this type of multiplexor is documented (Farina, Hubbard, and Lefkowitz, 1983). Proposals have been made for a multiplexor utilizing coherence multiplexing. With this approach an encoder is used to read the position of an optical code plate or the switches in a parallel binary format. Each channel is delayed with respect to the others by use of fiber optic delay lines and the data combined onto a single fiber. A phase-carrier, coherent detection scheme with a limited coherence laser is used to multiplex the information onto a single fiber. The advantages of the coherence approach are shorter delay lines and reduced mode system losses. Research on coherence multiplexing is documented (Glomb, 1986).

Fiber optic sensors are increasingly being considered in aeronautical design. Fiber optic length monitors can measure strains (elongations and compression) from 0.1 micrometers to 1.0 millimeters. Fiber optic acoustic area monitors can detect structural damage. These developments compensate for some of the difficulties anticipated as composite materials are increasingly used in aircraft structures. Some of the research and development that justifies the use of fiber optic sensors in aeronautical structures is documented (Otaguro, Michal, and Watanabe, 1986).

Quality control for brittle materials has used proof testing methods and analytical formalism as techniques for validation. These techniques involve subjecting the structure to applied loads much larger than expected service loads for short time periods. Measurements of flaw size can be used to estimate structural life under related conditions. These techniques assume that in-service stress distribution conditions are identical to proof testing conditions. No allowance is made for in-service wear, damage, or age. Safety considerations are factored in by the process of structural over-design. Fiber optic sensors are essentially glass or plastic fiber waveguides with small encircling spools. These sensors can be used to detect low amplitude acoustical signals. While several techniques exist for detecting the occurrence of acoustical signals in the structures containing the sensors, the techniques rely on two basic concepts:

- Measuring the resulting cyclic change in velocity of the optical signals in the fibers of the sensor (interferometric method).
- Measuring the change in propagation intensity in the fiber due to acoustic signal mode mixing.

The interferometric method is used in passive sonar device technology, i.e., submarine detection. Similarly, the interferometric method can be adapted for detection of acoustic emission from strained composite structures.

The acoustic sensor system would be designed as a network of sensors and built into the aircraft's composite structure. The glass fibers would be glued to the internal surfaces of the composite structures. The networks would be connected by fiber communication links to a processor. The net-works would be the vehicle for sending the sensor signals to the processor. Time delay spectroscopy could identify the source of the signal to the processor; acoustic emission analysis would determine the development of flaws. A real-time evaluation of structural integrity would result from this system. The composite structure could be integrated with this "listening blanket" during proof-testing, and the proof-testing period could be extensive. The purpose of this would be to determine the suitability of the composite structure before major assembly. In addition to stress determination, fiber optic sensors can also be used, within certain constraints, as temperature and chemical detectors.

This basic technology is at hand. Fiber optic Sagnac and Mach-Zehnder interferometric sensors are being used to monitor strain. The integration of sensor development, acoustic emission analysis, and computerized evaluation of brittle material integrity is missing. With proper emphasis, an integration of control and structural technologies within the above guidelines could be accomplished early in the coming century.

### 4.2. Artificial Intelligence

Artificial Intelligence has been discussed earlier in this tutorial. In paragraph 2.4.1, AI was identified as one of the two elemental disciplines for developing avionic technologies. In paragraph 3.4.1.2 it was discussed as a catalyst for review of current aircraft certification procedures and regulations. AI is that branch of computer science which attempts to create intelligent computer systems that understand, reason, learn, and solve problems (Buckanin, 1984). AI can casually be categorized into three areas: expert systems, image processing and interpretation, and natural language communication. In paragraph 3.4.1.2, the expert system category was defined and examples were given. In this section emphasis will be on the other two categories. Voice Command Processing (VCP) is an example of the natural language communication aspect of AI. Machine Vision (MV) (See paragraph 4.2.2.1 for definition) is an example of the image processing and interpretation category. Both of these examples have potential application in tomorrow's aircraft. VCP is considered to have a wide range of application; MV is more restricted.

#### 4.2.1. Voice Command Processing

VCP will have a major impact on how the pilot of the future commands and controls his aircraft. However, the integration of this technology with a future cockpit poses many difficulties, both in the hardware and system interface areas.

#### 4.2.1.1. The Need for Voice Command Processing

As the complexity of avionic systems increases, so does the workload on the pilot. This is a concern to both the civilian and military aspects of aerospace. The concern is most acute for today's high performance military aircraft that must perform single-seat tactical missions. The hands busy eyes busy mission pushes the limits for both pilot and aircraft. VCP is part of the solution to this problem; it should reduce the button and switch effort significantly. Developments in recognizer/synthesizer hardware and in recognition algorithms have made this technology one that should provide near-term benefits.

Boeing's entry in the next generation of subsonic transports, the Boeing 7J7, will utilize a voice recognition system. The USAF is testing voice activated electronics for its C-135C transport and its advanced F-16 fighter. These systems will respond to inquiries regarding fuel level, weapons status, and navigation; they will be responsive to numerous commands, e.g., changing radio channels and target proximity. There are over two-hundred basic information arrangements (pages) in the F-16C; each of these has numerous permutations and combinations. ATF will have hundreds of pages. *If a conventional display* approach is taken in the ATF, the pilot-aircraft interface will be impossible. Speech and hearing are two highly efficient forms of communicating. Systems oriented to their use must be developed for command and control.

4.2.1.2. The Problems for Voice Command Processing

Speech recognition is the process of correctly translating human speech into digital data. Speech synthesis is the reverse procedure. The latter is a mature technology: digital images of known responses can be stored and used when needed. Speech recognition is less developed. The sound of a given word may vary for the following reasons:

- Voice quality and attributes of the speaker.
- Context in which word is used.
- Inconsistent separators between words.

For a pilot, the sound of a given word may also vary for these reasons:

- Stressful conditions.
- Noise of aircraft.
- Presence of an oxygen mask.
- Altered g forces.

This difficulty is minimized by (1) requiring that speech be in isolated words, (2) limiting the acceptable vocabulary, and (3) programming the computer to recognize a single user. The imposition of the constraint that only isolated words be used will be accomplished with the definition of the command language. The pilot must be thoroughly trained in this language, and some type of video prompt should be present in the cockpit. The acceptable vocabulary is being limited. It is estimated that a vocabulary of between 200 and 500 words will suffice for even the most sophisticated systems. Programming the computer to recognize the pilot's pronunciations will be discussed later.

### 4.2.1.3. A Procedure for Voice Recognition

Figure 4.2-1 is a schematic for the voice recognition process. The audio input drives this process. There are three steps in voice recognition: extracting words out of the audio input, pattern recognition, and context analysis. The first step is that of extracting words out of the audio input. This consists of (1) converting the audio input to a spectrum and (2) extracting the spectral data. The conversion is normally handled by a Texas Instruments special purpose chip TMS320. This chip is a very fast 32-bit microprocessor that develops an energy distribution of the spoken word(s) by time. The extraction may be handled by such techniques as linear predictive coding, fast Fourier transforms, or digital spectral analysis. Linear predictive coding performs a polynomial fit on the sound spectrum; fast Fourier transforms develop frequency spectrums; and digital spectral analysis results in a series of attributes that characterize the primary frequencies of speech during each segment of time.

The second step is pattern recognition. This step utilizes the output of the first step and a library of relevant words. Depending on the technique used in the first step, one of the following will be produced:

- A set of coefficients representing the waveform.
- A frequency distribution of the waveform.
- A set of attributes of the waveform.

The library of relevant words is encoded in the same format as the output of step one. Assuming that digital spectral analysis is the extraction technique, the output of the first step may consist of attributes such as, the frequencies of each major frequency band or peak in the spectrum. These frequencies are referred to as formants. The library would contain the formants for different relevant words; there would probably be multiple formants per relevant word. Each formant is used as a "template" and is passed over the incoming sound message (output from the first step). The analysis continues until as much as possible of the incoming sound message is identified.

The third step is context analysis. Once the identification of individual words or phrases, is complete, the intent of the entire message is determined. This may be accomplished by graph analysis or encoded tables. The context analysis may be very efficient and permit only known words, or maybe very user-friendly and permit unknown words. Some known words may even be optional. The output of this step is the recognized pilot command. While not a function of voice recognition, the next step is interpretive logic that will obey the command.

The library of relevant words is developed during the programming process. This is a special mode of operation to the VCP. In this mode the pilot will identify a word to the VCP. The pilot will then pronounce the word under different circumstances. The system will then be tested under actual flight conditions. If there are pilot messages that the system does not recognize, the training mode will be reentered in an attempt to reproduce these conditions. Usually, a number of iterations through the training and actual flight cycle will be

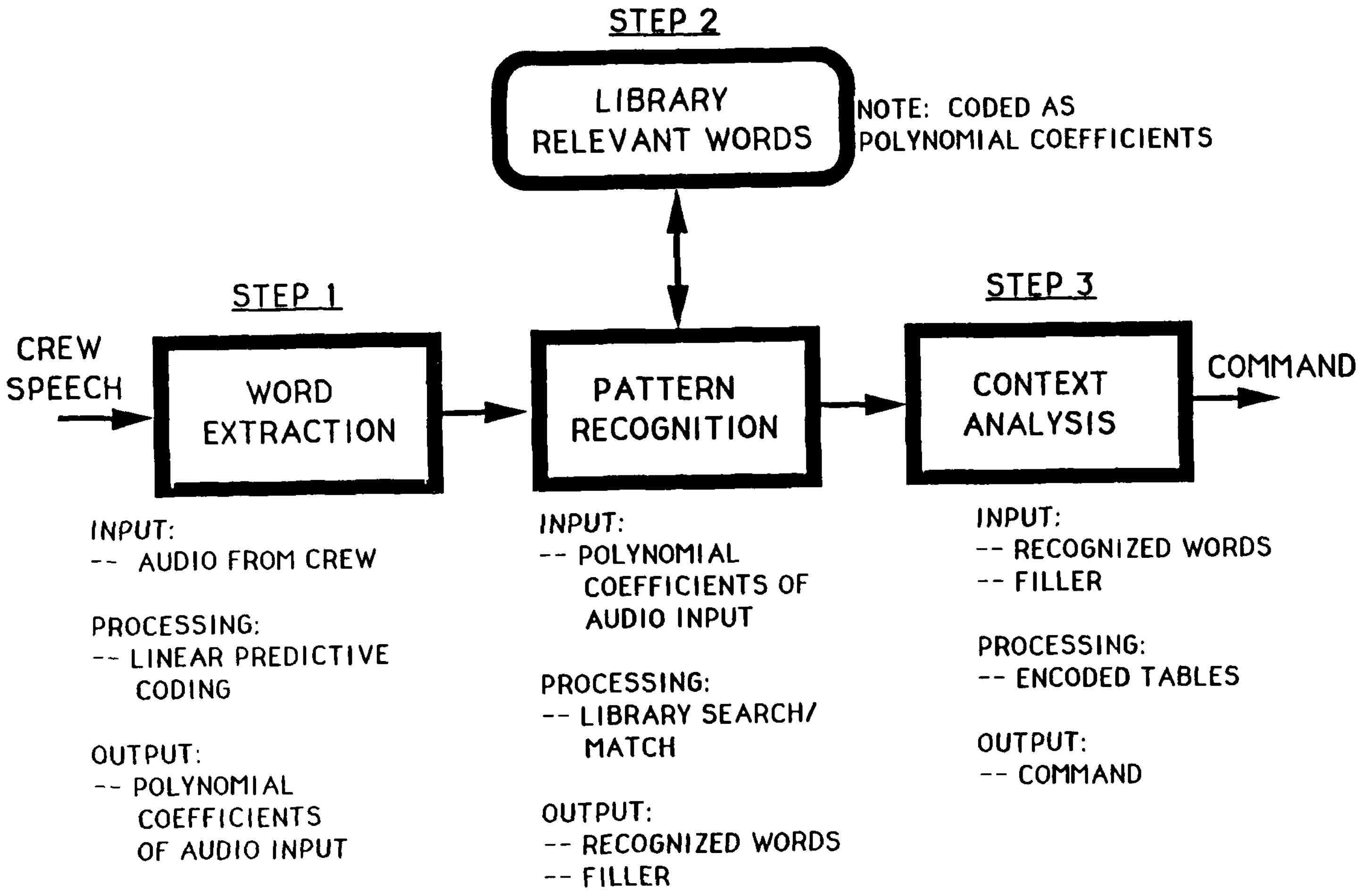


FIGURE 4.2-1. VOICE RECOGNITION SYSTEM

required. It is possible to have multiple libraries for a given aircraft, one for each potential pilot.

### 4.2.2. How Machine Vision is Accomplished

Machine Vision is used in the early stage (analysis stage) of research and development. It commences with the digitizing of the subject's image. An area is scanned by conventional or structured light beams. A charge-coupled camera or TV camera converts the image of the area being scanned into an array of picture elements (pixels). The intensity of light at each pixel is encoded as a binary number; this number represents a tone on a gray scale. Following the scanning and encoding, the array of pixels must be analyzed; it is at this point that most procedures for vision processing differ.

If the application is simple, such as the inspection of pieces, the pixel array is organized into dark and light segments. This process is called "thresh-holding". From this process, edges will be determined and shapes outlined. A library of standard shapes is used to determine the identity of the subject scanned. If microcircuits are being inspected, the library of shapes will be oriented to connections between circuit lines. If the scanned subject has edges that produce another topology, it may have flaws or breaks.

The analysis stage may be very simple, repetitive calculations on pixels or groups of pixels. Computers with simple Von Neuman architectures may find this an exhaustive job when the pixel density is high and/or the area scanned is large. This is an ideal application for parallel processors. Vision processing will encourage the development of parallel processing computer architectures.

*Inspection is a simple example of MV.* The hardware would consist of the camera system and a processor. Robotic vision, while having more hardware, is not necessarily more complex. A common application is locating an object that the robot will act on. For example, the vision system may find a particular spot on a circuit board where the robot is to insert a component. In this case, simple silhouettes may be sufficient for a program to identify a part by area, length, number of holes, or other features.

Surface curvature poses a problem to vision systems. Curvature may cause variances in reflection that are normal; this makes identification more difficult. An algorithm has been developed to handle this problem. The variations in light intensity are determined with scans moving in different directions. Reflection intensities resulting from surface curvature will vary from scan to scan; reflection intensities from flaws will not vary. When robotic vision requires great precision, 3-D vision may be required. A procedure used for 3-D vision is to utilize a single camera for illumination of the scanning beam and an additional camera(s) for a triangulation at the scanning spot. Robots have drilled holes in parts to a precision of 0.005 inches using this technique.

#### 4.2.2.1. Machine Vision in Aircraft

Because the flight environment for civil aircraft is reasonably structured, these aircraft have ways of "seeing" that do not conform to traditional concepts of vision. For tactical military aircraft, the flight environment is not so structured. Most of the aeronautical research and development in MV is for military aircraft. The DOD is currently studying the problem of applying MV to target recognition and navigation. One project calls for the recognition of a target by an aircraft or incoming missile; another project calls for the cross-country navigation of a high speed vehicle. Success in research as ambitious as this may be more than a decade away. On a simpler level, MV is successfully being used in factories to ensure the quality of manufactured electronics components. It is also being utilized to improve the quality of robotic welding, drilling, and cutting.

### 4.2.2.2. Two Complex Applications of Machine Vision

Target recognition is an advanced application for MV. The major problem is that of distinguishing between a tank and a truck when either vehicle may be viewed from any perspective (angle). The fact that the background for the subject being identified is undefined complicates the problem. Pattern recognition algorithms are being applied to this problem. In general, pattern recognition is to have a predefined image of the subject(s) for which identification is desired. This predefined image is then superimposed throughout the scanned area to determine whether or not it is present. For a single item, it would be necessary to superimpose the images from all perspectives throughout the scanned area. Other difficulties result from the following:

- The predefined images will vary as the elevation and distance of the scanning camera changes.

- The basic subject may not be fixed; e.g., the tank may have its gun pointed in any direction or the truck may be loaded/unloaded.

Synthetic discriminant algorithms are also being considered for target recognition. With this approach, a subject is defined to be a combination of a number of abstract geometric objects. The tank may be identified by the treads. This alleviates the problem of concern for orientation, but intensifies the problem of isolating the object from the background.

Another complex application is ground vehicle navigation. In this research, a vehicle with MV is to be driven over a winding road. The processing commences with a gray scale image of the road. Edges in the image that were parallel and approximately the same distance apart as the preceding image were taken as the road edges. Shadows and trees pose major problems. Color cameras reduce this problem as light intensity is used as a parameter for isolating the road from the remainder of the scanned area.

Obstacle avoidance is another facet of the navigation problem. Since this involves a distance dimension, a 3-D approach using lasers, sonar, or camera triangulation is being attempted. The success of this effort varies as to the ability of the obstacle to reflect sound. In addition to using a single detector (laser, sonar, or camera), research is underway to utilize all three sensors and have a master program compare the data submitted by the processor controlling each sensor (vote-taking). This data is coordinated with background data (images supplied by a satellite) to create the final computer image.

Progress in both target recognition and navigation is slow; however, MV is being used in manufacturing and domestic applications.

## 4.3. Computer Technology

Aircraft have become increasingly dependent on computers for both performance and safety improvements. This technology has grown by a factor of 10 every 5 years for the past 35 years; continued growth is anticipated. This rapid growth has primarily been the result of mammoth breakthroughs in device technology: vacuum tube to transistors to integrated circuits. Numerical software has also been greatly improved.

### 4.3.1. Advances in Microelectronic and Component Technologies

Since advances in these technologies have been a root cause of the evolution of today's digital avionics hardware, this subject has been alluded to in earlier sections of this tutorial. By the early 1990's it is anticipated that microelectronics will achieve today's recognized limits for Very-Large-Scale Integrated Circuits (VLSIC). Currently, Field Effect Transistor (FET) geometry cannot be scaled below approximately 0.25 micron. The reduction in the feature size of microelectronic devices will level off before reaching this limit. New techniques must be developed. As mentioned in section 2.4.5, 3-D architectures are a potential solution. These architectures would permit vertical as well as horizontal element interconnections. If problems such as heat removal can be solved, this technology may help sustain the reduction in feature size. An alternative to vertical interconnections is a reduction in the number of interconnections. This can be accomplished by developing modular digital function devices that accomplish more complex functions. More complex function devices is a second potential solution. A third possible solution is a new digital integrated circuit technology that uses submicron structures and new physical principles to solve the interconnect problem.

On the component level, rapid advances in processing and storage device technology are expected to continue. Logic and memory component density is expected to continue to increase by a factor of ten every five years for the next decade. As feature size converges to the 0.25 micron range, manufacturing chip cost will level off and, perhaps, increase. The cost per unit capability should continue to decline because of the increased functionality of the chip. Mass storage density has increased by a factor of four every five years. Current optical storage technology increases storage by a factor of 10 over current magnetic storage per unit volume. The utilization of video storage is also being studied for its adaptability to digital systems.

The "splitting" problem of optical bus systems is being researched. Optical bus systems that support in excess of 64 taps per kilometer are envisioned. In paragraph 4.1.2 of this tutorial, frequency division multiplexing techniques for optical fibers (permitting up to 50 channels per optical fiber) were discussed. Each channel has a bandwidth of 0.5 to 1 gigabit per second.

Single devices housing solid-state sensors, processors, and memory are anticipated within the next decade. As mentioned earlier, new chip-level and wafer-level interconnection technologies will be used to alleviate the component interconnection problem. Holography is an example of a new interconnection technology.

### 4.3.2. Advances in Parallel Processor Organization

The traditional processor architecture, the von Neumann architecture, is characterized by sequential operation. The processor's cycle time is the limiting factor on performance. The cycle time is bounded by the propagation time of signals. The propagation time of signals inhibits clock periods shorter than one nanosecond. Theoretically, the maximum achievable performance is one billion ($1.0^{+9}$) instructions per second. A parallel architecture is required if this limit is to be significantly passed. By the year 2000, effective parallel architectures consisting of thousands of processors, high bandwidth communications, and parallel structured software is anticipated.

Parallel processing is simple. In sequential processing, all data is accessed from a central data store. A processor that is working on several applications will spend most of its time retrieving data instead of calculating. In paragraph 4.2.2.1 of this tutorial, MV was seen to be an application that consisted of many disjoint tasks. This application is very conducive to implementation in a parallel environment. Each task would be performed on a subprocessor with its own memory.

If a microprocessor can perform thousands or tens of thousands of operations per second, a parallel machine with thousands of microprocessors could perform millions or tens of millions of operations per second. If the microprocessor costs $50, a parallel architecture of 1000 microprocessors would cost $50,000. A supercomputer with similar capacity would cost $10 million.

There are three major difficult steps to implementing parallel processor architectures. The first step is to develop the capability for a meaningful, efficient communication between many processors. This includes the responsibility of controlling several processors working on different tasks on the same problem. The second step is to simplify programming in a parallel environment. The third step is to develop parallel-oriented solutions to problems. The following two approaches for resolving the difficulties of these steps are being studied:

- Utilizing a single instruction/multiple data stream architecture (one sequence of instructions carried out in parallel on data).

- Utilizing a multiple instruction/multiple data stream architecture (many sequences of instructions carried out in parallel on data).

The multiple instruction/multiple data stream architecture is the purest form of parallel processing but offers the greatest challenge. Within these two broad groupings, parallel architectures can be subgrouped by grain size, degree of connection, shared memory, and the technique for decomposing a problem into subproblems that may be solved in parallel. Grain size is defined to be the degree of parallelism. An architecture with a few large processors (up to one hundred) has a large grain. An architecture with thousands of small processors has a small grain. The degree of connection relates to the interconnectivity of the processors. An architecture that has all processors communicating with all other processors has a high degree of connection. If processors can only communicate with a small, restricted set of processors, a low degree of connection exists. The shared memory attribute relates to whether all processors share a single memory store or whether each processor has its own memory store. The problem decomposition attribute relates to whether the machine decomposes the problem into tasks that may be executed in parallel or whether a programmer must do this.

NASA's Massively Parallel Processor (MPP) is an example of the first generation of parallel architectures. The MPP was developed by Goodyear Aero-space. The MPP is a small grain machine: 16,268 processors arranged in a 128 X 128 square. It has a low degree of connectivity. Each processor is connected to its four nearest neighbors. Every processor has its own 1,024 bits of memory. Problem decomposition is the responsibility of a programmer. A processor consists of a logic unit, an arithmetic unit, 35 shift registers, and the memory. A processor works on a single bit of data per executed instruction. All processors simultaneously could process 16,000 bits of data per cycle; a conventional mainframe processes 64 bits per cycle. Since each processor can execute 10 million instructions per second, the MPP maximum computing rate is 200 Million floating-point operations per second (Mflops). This rate is comparable to the Cray supercomputer.

The MPP is primarily performing signal and image processing. These applications are conducive to the nearest-neighbor connection scheme. The MPP outperformed the Cray by a factor of five. In the area of physics, plasma and gravitational field simulations are being attempted. These simulations are not as conducive to the nearest-neighbor connection scheme as are aerodynamic simulations such as image and signal processing.

NASA-Ames and Yale University have received two iPSC parallel machines. The iPSC was developed by Intel. The iPSC contains 128 processors, and would, therefore, be classified as a large grain machine. Each processor has over 512 kilobytes of memory. A hypercube design was used that interconnects each processor to seven neighbors. Thirty-two and sixty-four processor models of the iPSC permit each processor to connect with five and six neighbors, respectively. Problem decomposition is again the responsibility of a programmer.

Programming a parallel processing computer is very difficult. The four approaches being studied as potential solutions to this problem are as follows:

- Developing functional programming languages that automatically translate into a parallel algorithm.

- Developing process definition languages that permit a machine to dynamically allocate resources.

- Retrofitting parallel-oriented statements into a traditional algorithmic language like FORTRAN.

- Developing tools that permit a programmer to allocate resources in a simple manner.

A dataflow approach is the partitioning of a problem into a sequence of serial and parallel tasks which may be performed by separate processors. Dataflow processors are dedicated processors that allocate these tasks to their subprocessors. A program incorporates certain statements that define the route that data must follow and the transformations that occur to that data enroute. Using this program, the dataflow processor then assigns work to sets of processors. A nondataflow processor will only perform the work assigned to it.

### 4.3.3. Advances in Distributed Processor Organization

Distributed processor organization involves the arrangement of multiple processors into a network interconnected by some telecommunications medium. The growth of distributed computer system architectures has parallelled the growth in microelectronic technology. The result of microelectronic technological advances increased the importance of small computers. A network of small computers with a distributed workload could perform certain applications more reliably, efficiently, and economically than a single large computer with point-to-point communication to terminal devices. FCS's can be developed using distributed architectures. Paragraph 4.1.1 of this tutorial discusses the components of a FCS. The following discussion uses the FCS as an example of a distributed computer system. The architecture presented here is based upon the Bendix Multicomputer Architecture for Fault Tolerance (MAFT). "Fault-Tolerance in Distributed Digital FBW FCSs" (Gluch and Paul, 1986) covers this subject in great detail.

Figure 4.3-1 is a schematic of a FCS. From this schematic it is obvious that multiple processors are interconnected by a telecommunications medium, a trunk, or bus. The Primary Flight Computer, Secondary Flight Computer, Actuator Control Electronics, Data Sensor Units, and Autoflight Computer are all intelligent devices. They are all microprocessor-based units including memory, data store, and software. The bus may be electrical or fiber optic. Competition for the bus between intelligent units must be regulated by a protocol. A Carrier Sensed Multiple Access (CSMA) or token passing protocol may be used. With the CSMA, each of the nodes on the bus has a guaranteed window within a predetermined Access Time Interval (ATI). A node is a connection from an intelligent unit to the bus. In order for the FCS to perform adequately, the ATI must be small, perhaps on the order of 10 milliseconds. A token passing protocol requires that a token constantly circulate on the bus; only the node with the token may transmit.

Three types of data sensor units represent nodes on the bus. The pilot interface unit receives analog inputs from pilot controls, converts these to digital signals, constructs the appropriate communication layers, and places the resultant message on the bus during the alloted ATI. The appropriate actuator control electronics unit will take the message off the bus and act on it. Other nodes, such as the primary and secondary flight control computers, may also receive copies of this message, but for other purposes. An appropriate response may be returned to the originator and/or other interested parties by

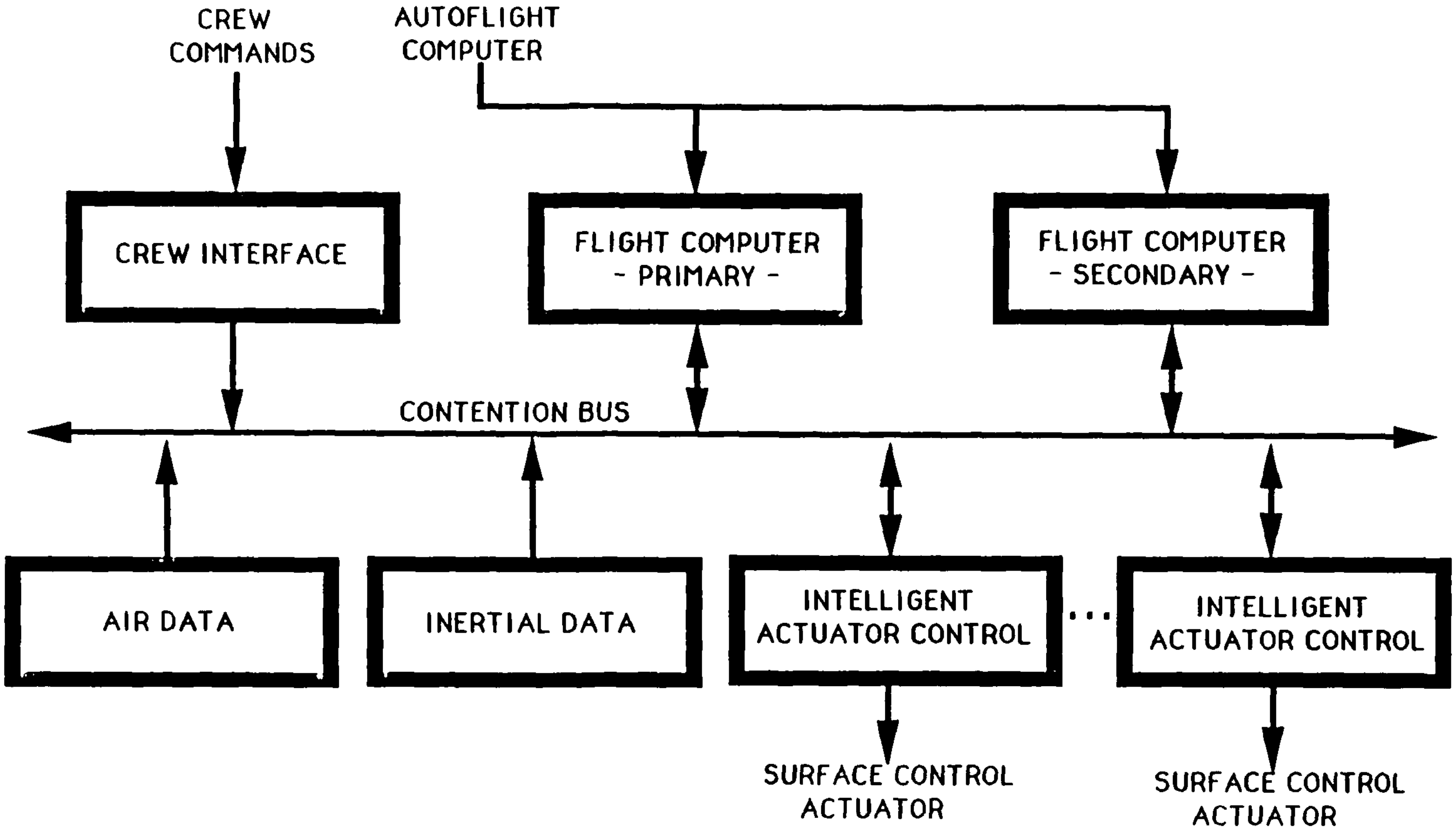


FIGURE 4.3-1. DISTRIBUTED PROCESSOR FLIGHT CONTROL SYSTEM

any recipient. In a similar manner, air data and inertial data sensors will broadcast data across the bus during their ATI. This data will be received by the autoflight computer, the primary flight computer, and the actuator control electronics units. The autoflight computer is responsible for determining whether flight sensors are recording flight parameters that meet projections. If not, surface control commands may be issued to correct the situation.

Actuation control of the surfaces and interface to the bus is accomplished by the actuator control electronics units. These intelligent units may interface to either semi-electromechanical or hydraulic actuation systems. These units perform closed loop control, low frequency equalization, fault detection, and reconfiguration services for each of the control surfaces.

The architecture depicted here represents a highly distributed approach to the implementation of a digital FBW system. Intelligent processing units located throughout the aircraft work collectively through communications provided by a multi-access bidirectional bus. While the overall system functions are distributed, the hardware and software of the primary flight computer is the central ultra-reliable LRU in the system. Reliability concerns dominate the system. The probability of system failure must be virtually zero. Multiple hardware redundancy is employed. This redundancy involves multiple communication busses, sensors, flight control processors, and actuators. Additionally, there will be redundancy in all software modules. All intelligent systems will incorporate fault-tolerant logic.

## 4.4. Advances in Control and Display Technologies

As the number and complexity of avionic systems grow, it becomes increasingly difficult for the aircraft crew to assume all past responsibilities, as well as the workload resulting from the new systems. With computer-driven surface controls providing stable flight in inherently aerodynamically unstable aircraft, the pilot is no longer the operator of the aircraft, but is rapidly becoming a flight monitor/manager who will intervene in the event of system failure. There are two directions that future systems may take. First, systems may be designed that would augment the operator's information acquisition and processing capabilities. Second, the systems may be designed to eliminate the need for operator intervention on the flight deck.

### 4.4.1. Improved Man-Machine Interface

The explosion in numbers of avionic systems has resulted in extremely large volumes of data being present on the aircraft computers. The crew may not view all of this data; however, sufficient data to permit the crew's full awareness of the aircraft's situation is important. Information from onboard sensors, stored knowledge, and observation/interaction of the crew must be digested and presented in a manner that is not overwhelming. The crew must focus on the decision process, strategy development, and strategy implementation.

#### 4.4.1.1. Short Range Cockpit Improvement

The A320 cockpit bears limited resemblance to its predecessors, but one that may be a future trend setter. Roll and pitch controls are allocated to "side sticks" that are installed on lateral consoles. The conventional control column is no longer present. In conventional aircraft the control column function required large mechanical assemblies that occupied much of the subfloor compartment. The sidestick controller uses analog displacement sensors to permit large grip motion, instead of force sensors that would restrict motion. The sidestick controller includes roll and pitch sensor boxes and centering "feels". A solenoid-operated detent locks the control lever at neutral when in autopilot mode. The stick does not respond to autopilot commands The canted hand grip has maximum angular deflections of 16 degrees in pitch and 20 degrees in roll. The sensors detect displacements of the hand grip; this results in the transmission of analog signals to the FCS computers. All roll and pitch control is under the guidance of the fully electronic FCS.

Minimal mechanical backup is provided by a mechanically controlled rudder and standby tailplane trim. The basic yaw control uses a single rudder controlled from the cockpit pedals. A trim switch is located at the rear of the central pedestal and controls rudder trim.

Another recent innovation in today's cockpit is the presence of CRT displays. Usually, one set of CRTs displays traditional flight control mode information, as well as consolidations of artificial horizon, horizontal situation indicator, and airdata instrumentation. Another CRT displays integrated plan and profile views of the projected flight plan.

Smart flat panel displays are being considered as potential replacements for CRTs. Examples of the technologies being considered are gas plasma, liquid crystal, and thin film electroluminescence. The Liquid Crystal Display (LCD) is getting particular attention because of its low power and low voltage requirements. It has the disadvantages of poor temperature performance, low dynamic range, and limited viewing angle; however, these problems are solvable. Research with thin-film transistor LCD matrix devices has established the LCD technology as the most likely successor to the CRT.

4.4.1.2. Long Range Cockpit Improvement

Whenever a new avionic device is placed in the cockpit, more visual workload is placed on the pilot. Researchers working on the virtual panorama display, a precursor of the USAF Supercockpit Project, are attempting to estimate the workload produced by a new display before the display appears in a cockpit. This involves creating semantic networks from the information content in an image. A path is created in the network connecting a certain piece of information in the image with information known to the pilot. The number of semantic nodes that must be traversed are used as a measure of the workload placed on the pilot by the image. This technique has been tried in simulated missions, and the simulation confirmed the technique. The more complex the semantic network rating, the greater the deterioration in pilot performance in the simulated mission.

In the supercockpit the pilot will wear a helmet weighing approximately three and one-half pounds. Two tiny video screens will be mounted in front of the pilot's eyes. These screens will enable the pilot to view avionics displays, as well as magnified and illuminated real-world scenes. The data to be viewed will be selected by the pilot, or the FCS will display data on an exception basis.

In the supercockpit, the screens will be translucent, so the images will be projected on the real world. A flight simulator helmet from which the supercockpit helmet will evolve utilizes two tiny CRTs; each CRT projects a scene one thousand pixels wide and one thousand pixels high, each pixel has a width of approximately twelve microns. The concept of the translucent display, instead of the CRT, is being tried in the Army's developmental LHX helicopter. There is concern over pilot confusion resulting from superimposing the display images on the real world. Research has shown that simulated images cause little confusion; whereas, actual images (such as magnifications) may cause considerable confusion. A 14-bit precision system is used to detect the orientation of the pilot's head. If the pilot turns his head, the display image will rotate with his head in relatively the same position. The system uses a set of three orthogonal radio-frequency coils mounted in the cockpit and three tiny magnetic detectors mounted in the helmet. Signals from the detectors are used to determine the exact position of the helmet. Special purpose electronics were developed to compensate for distortions in the optical system. These electronics result in (1) the blending of edges when there are two overlapping optical fields, and (2) the creating of the effect of tunnel vision.

If the scene becomes overly complicated, some of the data may be fed into the pilot's ear. The speakers would be located in the pilot's helmet. Locations of nearby aircraft may be indicated by sounds located in virtual or apparent space around the pilot. Techniques for localizing sound are primitive. Stereo indicates the lateral location of sound (left or right), but doesn't localize it in the two remaining dimensions, up/down or front/back. The cues used in stereo (timing, phase shift, and loudness difference between the ears) are important, but are incomplete. Paragraph 4.2.1 of this tutorial discussed VCP. Audio sensors for picking up the pilots' speech would also be present in the helmet.

Pilots can be overloaded with sounds, as well as sights. With VCP the voice can be used to control the aircraft. The sense of touch can also be used. In the cockpit of the future, the pilot may be able to reach out and touch a "virtual switch" to activate a sensor. The switch may be an image from his helmet. This may be accomplished through fiber optic technology or by having a pneumatic device built into a special glove. Far more sophisticated pneumatic arrays using piezoelectric materials may be able to simulate the touch of any object.

4.4.1.3. Pilot Associate Program

Developments in AI will have a tremendous impact on future cockpits. AI Implications for Advanced Pilot/Vehicle Interface (PVI) Design (Maxwell and Davis, 1985) is an excellent source on the methods and extents to which AI will effect the PVI in future generation aircraft. Avionic systems are proliferating in today's aircraft. This has been particularly a problem in military tactical aircraft with flight crews of one or two persons. In this case, flight crews are facing rapidly increasing workloads which must be accommodated under stressful conditions. As avionic systems increase in commercial and general aviation, the same effect will be felt for aircraft in these classes. The amount of data to be analyzed and pressures to reduce crew costs will increasingly reduce the role of the human crew in data analysis and decision-making. The PVI is that portion of the cockpit that presents information to the flight crew for their analysis, and receives control information from the crew. As the amount of aircraft data and control requirements have increased, PVIs have been designed to compensate in several ways.

First, multifunctional displays have been designed that do not display all data but only the data that is functionally relevant. Second, integrated displays are designed to provide cross-system data that is functionally related. Third, automated systems are designed that operate quasi-autonomously from the crew; by doing this, the crew needs only to monitor systems intermittently instead of continuously controlling them. Fourth, multifunctional systems are designed that permit crew controls at a high level; they do not have to give attention to subsystem details. The effect of each of these should be to reduce the workload on the crew.

Artificial Intelligence is a technology that offers the possibility of massive improvements in this area. The DOD Pilot Associate program is studying the feasibility of having a computer responsible for the routine tasks of flying, and acting as a copilot. Additionally, the pilot's brain waves and heart muscle electrical rhythms are monitored to determine "black out". If a pilot blacks out, the computer will completely take over flight of the aircraft. Figure 4.4-1 depicts a PVI utilizing an AI computer system. There are three relationships that may exist between a pilot and an AI system. AI Implications for Advanced PVI Design (Maxwell and Davis, 1985) discusses these relationships in detail.

The first relationship is the Pilot Manager/AI Associate model. In this model the pilot is responsible for those decisions at the outer control loop level. The pilot performs a systems manager function; the AI system responds to the directions of the pilot. Decisions in the inner control loop are the responsibility of the AI Associate. This model is acceptable in operational situations where tasks may be partitioned vertically. The pilot performs tasks at the upper end, while the AI Associate performs those at the lower end.

The second relationship is the Pilot/AI Colleague model. In this model the pilot works with the AI Colleague on the basis of equality and shared responsibility. Each oversees the actions of the other and contributes to the performance of virtually every task. This model is best suited to operational situations in which a vertical partitioning is either impossible or inefficient.

The third relationship is the Autonomous Assistant model. In this model the computer may actually assume control of the aircraft, and the pilot will be subordinate to the AI system. This relationship is desirable if the pilot becomes incapacitated to the extent that the pilot cannot function in one of the other two relationships.

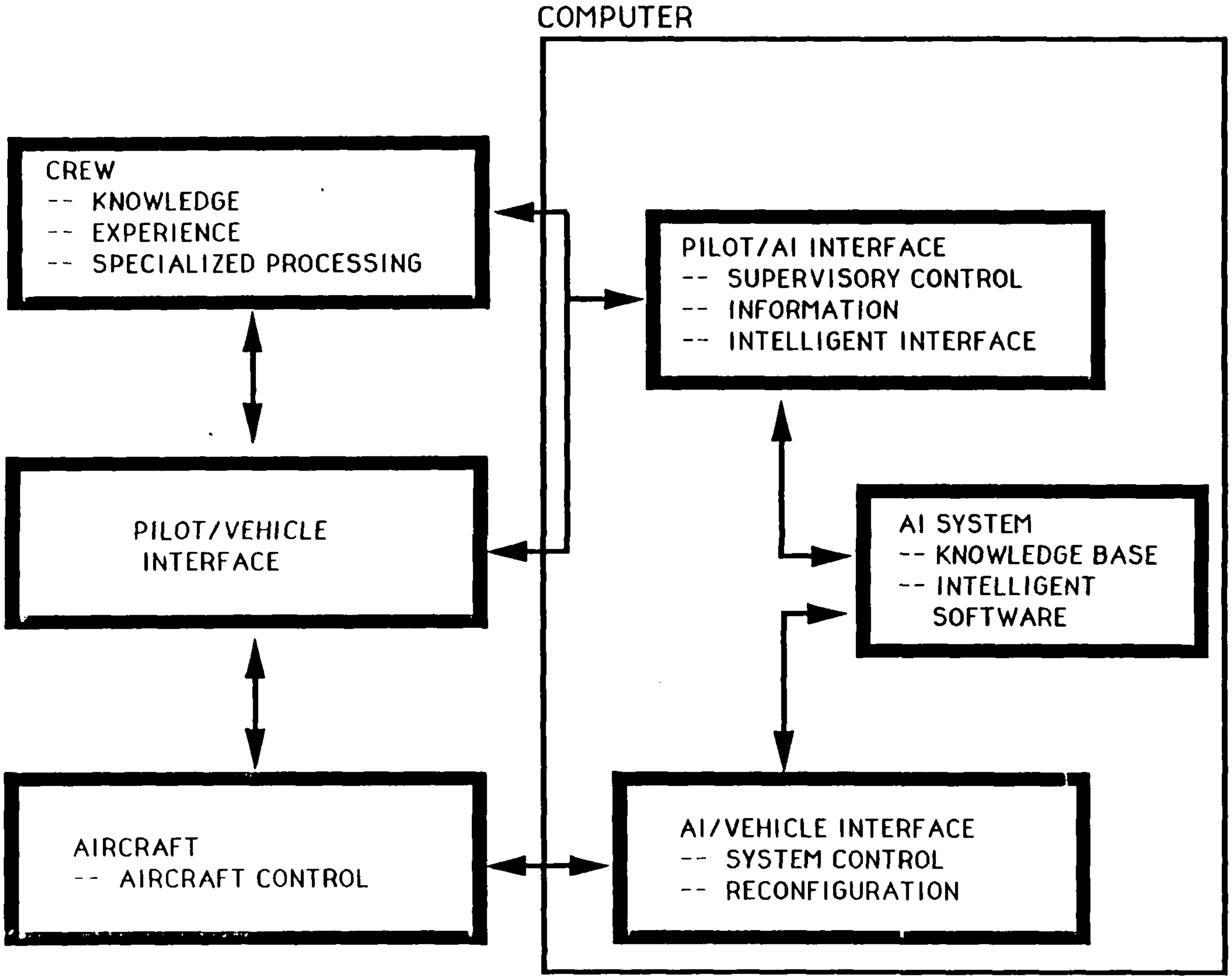


FIGURE 4.4-1. PILOT/VEHICLE INTERFACE WITH ARTIFICIAL INTELLIGENCE SYSTEM

These three relationships are not mutually exclusive. A single PVI may support all three relationships. During a single mission, each of the models may be used when operational situations dictate. The particular blend of the above three models into the design of a single PVI is determined by the characteristics of the tasks being performed and the problems being solved.

The technology for supporting such a PVI is far in the future. In addition to the hardware and software enabling technologies, design algorithms must be developed for resolving disagreement between the pilot and AI system, determining when the AI system should interrupt the pilot from his current task and enabling the PVI to change from one relationship to another.

### 4.4.2. Remotely Piloted Vehicles

With the exception of highly restricted applications, there appears to be no movement to eliminate humans from the flight deck. However, improved computer technology does enable autonomous and semiautonomous aircraft to be remotely piloted. This may be desirable when the presence of a human pilot is undesirable. Examples include vehicle missions that require very long endurance (e.g., space probes, communication relays, and fire controls) and military missions that are too dangerous for manned aircraft (e.g., defense suppression). When communication links may be sustained, the RPV may operate under the direction of a control station. In missions subject to the severance of communication links, the unmanned vehicle may have to operate autonomously. Autonomous operation is far in the future. The technology advances needed to support RPV development are intelligent sensor control, intelligent sensor processing, AI, communications, and remote control related devices.

### 4.4.2 1. Control of a Remotely Piloted Vehicle

Semiautonomous RPV must be controlled from a "mother" craft. The next generation of spacecraft will include several RPVs. Examples of these are the Orbital Maneuvering Vehicle (OMV) and the Orbital Transfer Vehicle (OTV). The NASA Space Station will be the "mother" craft. These vehicles will serve as supply carriers, service satellites, and propel missions into deep space.

The latest technology is being applied to controlling the OMV and OTV from the space station. Pilot video monitors provide navigational displays to the pilot. The primary video monitor will display the main video camera signal received from the RPV. The secondary video monitor provides overlays to the primary monitor; the selection of a particular overlay is at the discretion of the pilot. Information displays will provide the pilot with work aids and secondary displays. These include set-up programs, checklists, operating procedures, real-time flight trajectory graphs, and alarms. The information displays will most likely be a color microcomputer display. A control panel will also be present in the form of a microcomputer display; touchscreen technology will provide graphic representation of push-button panels and associated status information.

Hand Controllers provide the facilitv for manuallv maneuvering the RPV. Usually two controllers will be present: one for control of the X-, Y-, and Z-axis maneuvering and one for roll, pitch, and yaw maneuvering. These two controllers permit a six degree of freedom vehicle control. Touchscreen is the primary mode of control for function selection, but a keyboard and mouse may be used as a backup. An alternate mode of control is speech recognition and synthesis.

4.4.2.2. Avionics for a Remotely Piloted Vehicle

The preceding section discussed RPV control for a vehicle in a space application. Other RPVs may have to navigate the near-earth atmosphere at varying degrees of altitude. The avionics for such a vehicle would include flight control, inertial attitude reference, air data terminal, and payload/datalink systems. These are shown in schematic form in figure 4.4-2. At present, these RPVs are primarily used in military applications. As a result, the payload may consist of sophisticated weaponry with digital components or electronic countermeasures. The datalink is a secure communications system that supports the RPVs remaining at a safe distance from enemy defenses and maneuvering in a highly evasive fashion. The total cost of the RPV avionics would be concentrated in these two systems.

The FCS consists of a microprocessor with Random Access Memory (RAM) and/or Erasable Programmable Read-Only Memory (EPROM) memory. This processor handles the software functions associated with attitude stabilization, guidance, navigation, command execution, payload interface, datalink interface, and miscellaneous computational tasks. This microprocessor receives inputs from the flight sensor instrumentation and generates outputs to various servos and actuators. The inertial attitude reference is a sensor that provides accurate data on instantaneous vehicle rates. The air data terminal is the end of the data link on the RPV; it communicates with the control station.

Avionic systems represent approximately 80 percent of the cost of an RPV; the payload, itself, may represent 60 percent of the cost. Research and development effort is directed toward reducing the payload and ground control station costs. Since a major application for this type of RPV is target recognition, MV is an enabling technology for future RPV advances. (See paragraph 4.2.2.)

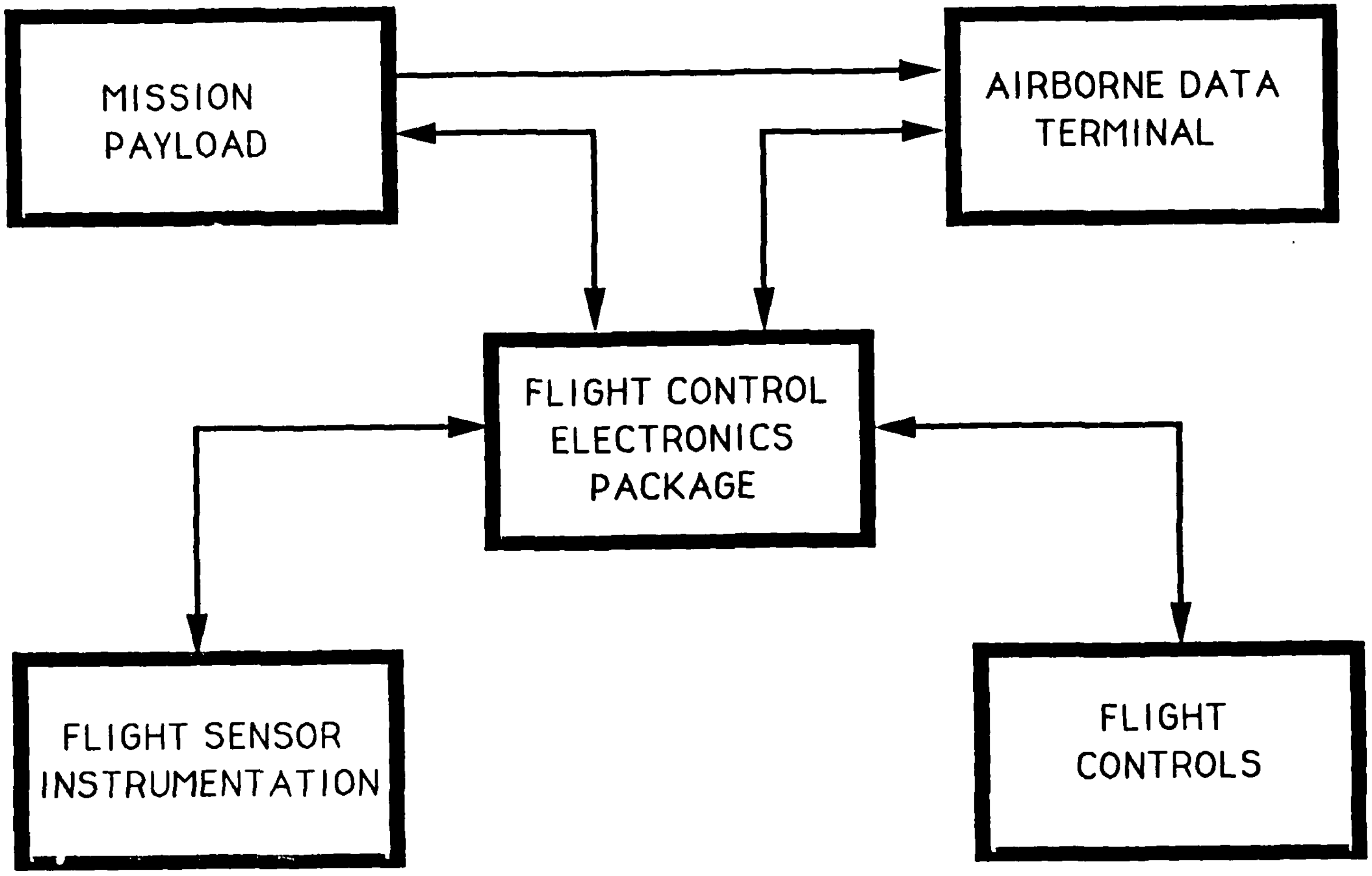


FIGURE 4 4-2. REMOTELY PILOTED VEHICLE AVIONICS

## BIBLIOGRAPHY

Aeronautical Policy Review Committee, Review of National Aeronautics Policy, Committee Report, November 1983.

Aeronautics and Space Engineering Board, Aeronautics Technology Possibilities for 2000: Report of a Workshop, 1984.

Brahney, J. H., "Certification Issues in Civil Helicopters," Aerospace Engineering, June 1988.

__________, "Moving Closer to Fully Integrated Control," Aerospace Engineering, October 1986.

__________, "Guidance, Navigation, and Control for 21st Century Aircraft," Aerospace Engineering, April 1986.

Buckanin, D. L., Artificial Intelligence: Overview and Annotated Bibliography," DOT/FAA/CT-TN84/5, March 1984.

Editor, "Fluidic Flight Control: Early Test Results," Aerospace Engineering, June 1988.

Editor, "Helping the Pilot Handle the Supercockpit," Aerospace America, February 1987.

Editor, "New Propulsion Concepts and FAA Certification," Aerospace Engineering, February 1988.

Epstein, A. H., ""Smart" Engine Components: A Micro in Every Blade?," Aerospace America, January 1986.

Executive Office of the President, Office of Science and Technology Policy Report, National Aeronautical R&D Goals - Technology for America's Future, March 1985.

Farina, J., R. Hubbard, and P. Lefkowitz, "Development and Test of a Digital/Optical Rotary Position Transducer, USAAVRADCOM TR 83-D-15 United States Army Research and Technology Laboratories, 1983.

Federal Aviation Administration Report, Aviation Technology - A View of the Future, Spring 1987.

Glomb, Jr., W. L., Passive Fiber Optic Coherence Multiplexing for Aircraft Sensors, IEEE/AIAA 7th Digital Avionics Systems Conference, 1986.

Gluch, D. P., and M. J. Paul, "Fault-Tolerance in Distributed Digital Fly-By-Wire Flight Control systems," IEEE/AIAA 7th Digital Avionics Systems Conference, 1986.

Hartley, C. S., and R. Pulliam, Use of Heads-Up Display, Speech Recognition, and Speech Synthesis in Controlling a Remotely Piloted space Vehicle, IEEE/AIAA 7th Digital Avionics systems Conference, 1986.

Lerner, E. J., "Many Processors Make Light Work," Aerospace America, February 1986.

Lupinetti, A., "Aviation Technology: A View of the Future," a viewgraph presentation, 1987.

__________, "Talking to Your Aircraft," Aerospace America, January 1986.

Martin, J., Design and Strategy for Distributed Processing, Prentice-Hall, Inc., 1981.

Maxwell, K. J., and J. A. Davis, Artificial Intelligence Implications for Advanced Pilot/Vehicle Interface Design, IEEE/AIAA 6th Digital Avionics Systems Conference, 1985.

Moore, C. A., R. D. Moore, and J. C. Ruth, Application of Voice Interactive Systems-Military Flight Test and Future, IEEE/AIAA 6th Digital Avionics Systems Conference, 1985.

National Aeronautics and Space Administration, "1986 Long-Range Program Plan," August 1985.

Otaguro, W. S., R. J. Michal, and S. F. Watanabe, Fiber Optic Monitors for Space Structures, IEEE/AIAA 7th digital Avionics Systems Conference, 1986.

Peterson, G. P., "Heat Removal Key to Shrinking Avionics," Aerospace America, October 1987.

Society of Automotive Engineers, SAE Committee AE4L Report No. AE4L-87-2, February 1987.

Terry, J. L., Tomorrow's Flight Controls: Helicopter Fly-By-Light, IEEE/AIAA 5th Digital Avionics Systems Conference, 1983.

Vandersteen, A. D., Avionics for the Small Remotely Piloted Vehicle, IEEE/AIAA 7th Digital Avionics Systems Conference, 1986.

## GLOSSARY

Ambient. The substance which absorbs heat from the heat sink.

Artificial Intelligence. The characteristics of a machine programmed to imitate human intelligence functions.

Autofeather. To automatically and swiftly feather the propeller when the engine fails to drive it.

Canard. A tail-first aerodyne, usually with auxiliary horizontal surface at the front and a vertical surface at the back.

Fly-By-Glass. Flight control system where fiber optics carry the signal.

Fly-By-Light. Flight control system where fiber optics carry the signal.

Fly-By-Wire. Flight control system with electric signaling.

Gigabit. One billion bits.

Kilobyte. One thousand bytes.

Micron. One-millionth of a meter.

Nanosecond. One-billionth of a second.

Thyristors. Solid-state devices that convert alternating current to direct current.

## ACRONYMS

| | |
|---|---|
| 3-D | Three-Dimensional |
| ACS | Automatic Control System |
| AERA | Automated Enroute Air Traffic Control System |
| AFM | Advanced Fuel Management |
| AI | Artificial Intelligence |
| ATF | Advanced Tactical Fighter |
| ATI | Access Time Interval |
| CRT | Cathode Ray Tube |
| CSMA | Carrier Sensed Multiple Access |
| DARPA | Defense Advanced Research Projects Agency |
| DFCS | Digital Flight Control System |
| DOD | Department of Defense |
| EIU | Electronic Interface Unit |
| EMI | Electromagnetic Interference |
| EPROM | Erasable Programmable Read-Only Memory |
| FAA | Federal Aviation Administration |
| FADEC | Full Authority Digital Engine Controller |
| FAFTEEC | Full Authority Fault Tolerant Electronic Engine Control |
| FAR | Federal Acquisition Regulation |
| FBL | Fly-By-Light |
| FBW | Fly-By-Wire |
| FCS | Flight Control System |
| FET | Field Effect Transistor |
| GaAs | Gallium Arsenide |
| GNC | Guidance, Navigation, and Control |
| HERF | High-Energy Radio Frequency |
| ITT | (Consultative Committee for) International Telegraphy and Telephony |
| kA | kiloamp |
| LCD | Liquid Crystal Display |
| MAFT | Multicomputer Architecture for Fault Tolerance |
| Mbps | Million bytes per second |
| Mflops | Million floating-point operations per second |
| MPP | Massively Parallel Processor |
| OMV | Orbital Maneuvering Vehicle |
| OTV | Orbital Transfer Vehicle |
| PCS | Primary Control System |
| PLA | Power Level Angle |
| PVI | Pilot/Vehicle Interface |
| RAM | Random Access Memory |
| RCA | Radio Corporation of America |
| RF | Radio Frequency |
| RPV | Remotely Piloted Vehicle |
| RTCA | Radio Technical Commission for Aeronatics |
| SAE | Society of Automotive Engineers |
| STOL | Short Takeoff and Landing |

| | |
|---|---|
| TCAS | Traffic Alert and Collision Avoidance System |
| TTL | Transistor-Transistor Logic |
| USAF | United States Air Force |
| USB | Upper Surface Blowing |
| VHSIC | Very-High-Speed Integrated Circuits |
| VLSIC | Very-Large-Scale Integrated Circuits |
| VTOL | Vertical Takeoff and Landing |

# GLOSSARY
# and
# ACRONYMS

# NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

# GLOSSARY

ABSORPTION LOSS. (11) Attenuation or retention of electromagnetic energy passing through a material, a shield. Absorption loss and reflection loss contribute to total shielding effectiveness (SE).

ACTION INTEGRAL. (13) The action integral is a critical factor in the production of damage. It relates to the energy deposited or absorbed in a system. This energy cannot be defined without knowing the resistance of the system. The instantaneous power dissipated in a resistor is $I^2R$ and is expressed in watts. For the total energy expended, the power must be integrated over time to get the total joules, watt-seconds. By specifying the integral of $i(t)^2$ over the time interval involved, a useful quantity is defined for application to any resistance value. In the case of lightning, this quantity is defined as the action integral and is specified as $i(t)^2dt$ over the time the current flows.

ACTIVE FAULT. (10) A fault that can produce an error (for some input) while executing the current program.

ACTUAL TRANSIENT LEVEL. (13) The actual transient level is the level of transients which actually appear at the system interfaces as a result of the external environment. This level may be less than or equal to the transient control level but should not be greater.

ADDRESSING CAPACITY. (6) The number of components addressable by the protocol used on a given data bus.

$\alpha$-FAULT. (10) A fault activated by the baseline program (see $\beta$-FAULT).

AIRCRAFT LIGHTNING INTERACTION. (13) An encounter with lightning that produces sufficient current within or voltages along an aircraft skin or structure to pose a threat to the aircraft electrical/electronic systems, as a result of a direct lightning attachment.

AMBIENT. (16) The substance which absorbs heat from the heat sink.

ANALYTICAL REDUNDANCY. (7) The use of software algorithms which use known mathematical relationships between different sensors for sensor failure detection and replace most of additional redundant sensor hardware.

ANALYTICAL ROOT SOLUTION. (4) Information obtained from the roots of the characteristic equations of the airplane model such as short-period or phugoid frequency response.

ANGLE OF ATTACK. (4) Angle between the longitudinal axis of an aircraft and the direction of movement.

ANODIZE. (11) A preparation by electrolytic process that deposits a protective oxide, insulating film on a metallic surface (aluminum). The oxide defeats electrical bonding. Alodine and iridite finishes on aluminum are conductive.

APERTURE. (11) An opening, such as a nonconductive panel joint, slot, or crack, allowing electromagnetic energy to pass through a shield.

ARTIFICIAL INTELLIGENCE. (16) The characteristics of a machine programmed to imitate human intelligence functions.

A-SPECIFICATION. (9) The highest level specification typically produced by the contracting organization to define a system (see MIL-STD-1521).

ASSURANCE ASSESSMENT. (4) Procedures whose purpose is to ensure that a proposed system functions according to design specifications.

ASYNCHRONOUS MESSAGES. (6) Electronic signals with transmission times that are not known a priori. These may include priority signals requiring immediate access to the bus.

ATTACHMENT POINT. (13) A point of contact of the lightning flash with the aircraft.

AUDIO FREQUENCY (AF). (11) The spectrum (20 to 20,000 Hz) of human hearing, often defined as extending from approximately 20 Hz to 50 kHz and sometimes to 150 kHz. Audio noise is nuisance hum, static, or tones from power line 400 Hz, switching regulator and digital clock harmonics, or HF, VHF transmitter frequencies.

AUTOFEATHER. (16) To automatically and swiftly feather the propeller when the engine fails to drive it.

AUXILIARY PROGRAMS. (10) Software executed occasionally.

AVALANCHING LATENT FAULTS. (10) The successive activation of latent faults.

BACKSHELL. (11) Metal shell connecting circuit shields or overbraid to an electrical connector.

BACKWARD RECOVERY. (9) Restoration of the system to some previous known correct state and restarting the computation from that point.

BALANCED CIRCUIT. (11) A signal, acting line-to-line, between two conductors having symmetrical voltages identical and equal in relation to other circuits and to ground. "Differential mode" is line-to-line; "common mode" is line to ground.

BANDWIDTH (BW). (11) Frequencies bounded by an upper and lower limit in a given band associated with electronic devices, filters, and receivers.

BASELINE PROGRAM. (10) A set of continuously executed software modules.

BENIGN FAULT. (10) A fault that cannot produce an error while executing the current program, regardless of input, but may produce an error for some other program.

$\beta$-FAULT. (10) A fault not activated by the baseline program (see $\alpha$-FAULT).

BIT TIME. (6) The time it would take to transmit one bit. Usually this is "blank" time when nothing is being transmitted. One nth of the bus speed (i.e., on a 1 kHz bus, the bit time is $10^{-3}$ seconds).

BLOCK TRANSFER. (6) A data transfer mode allowing the transfer of variable length data blocks.

BOND, ELECTRICAL. (11) Electrical connection at two metallic surfaces securely joined to assure good conductivity often 2.5-mΩ maximum for electrical/electronic units and 1Ω for electrostatic dissipation or safety. A "faying surface" bond maintains contact between relatively large or long surfaces. Inherently bonded parts are permanently assembled and conductivity exists without special preparation: such as with welding, brazing.

BRAID, OVERBRAID. (11) Fine metallic conductors woven to form a flexible conduit or cableway and installed around insulated wires to provide protection against electric fields and radio frequencies. Best when peripherally connected to backshells. A grounding strap/jumper may be made of braid.

BROADBAND. (12) A frequency spectrum which is wide compared to the bandwidth of the device used to detect it.

BROADCAST. (4) *Transmission of messages* to all terminals without reference to the identification of the receiving station or terminal.

BROADCAST CAPABILITY. (6) The capacity to transmit messages to all terminals simultaneously.

CABLE OR HARNESS. (11) A bundle of separate, insulated, electrical circuits, shielded or unshielded, usually long and flexible and having breakouts, terminations, overbraid, and mounting provisions completely assembled.

CABLEWAY. (11) A solid metallic housing (liner, foil, coating) surrounding and shielding insulated electrical conductors. Also called conduit, tray, or raceway. Crosswise or transverse openings or breaks in the metallic cableway cause noise voltages to be transferred to internal wire circuits.

CANARD. (16) A tail-first aerodyne, usually with auxiliary horizontal surface at the front and a vertical surface at the back.

CAT IIIa LANDING. (6) One of several landing categories defined in FAR 91. CAT IIIa implies the need for an instrument landing approach.

CENTRAL CONTROL. (6) Control from one master, whether stationary or non-stationary.

CHARGE TRANSFER. (13) The integral of the current over its entire duration, i(t)dt, in coulombs.

CHORD. (4) The straight line segment intersecting or touching an airfoil profile at two points.

COMMAND/RESPONSE. (6) "Operation of a data bus system such that remote terminals receive and transmit data only when commanded to do so by the controller." (MIL-STD-1553 Designer's Guide, 1983, p. II-3.)

COMMON MODE SIGNAL. (11) Identical and equal signals on input conductors or at the terminals of a device relative to ground.

COMMON MODE REJECTION. (11) The ability of wiring or an electronic device to reject common mode (line-to-ground) signals and maintain fidelity of differential mode (line-to-line) signals.

COMMON MODE (CM) IMPEDANCE. (11) Impedance or resistance shared by two or more circuits so that noise voltages/currents generated by one are impressed on the others.

COMPONENT DAMAGE. (13) Condition arising when the electrical characteristics of a circuit component are permanently altered beyond its specifications.

CONDUCTED EMISSION (CE) OR INTERFERENCE. (11) Voltage/current noise signals entering or leaving a unit on interface conductors. Emission is the general term, interference is undesired noise.

CONTENT ADDRESSING. (6) The system of identifying message recipients based on information embedded in the message. This is in contrast to destination terminal addresses.

CONTROL LAW. (7) The physical relationship between various sensors and control surfaces.

CORONA. (13) A luminous discharge that occurs as a result of an electrical potential difference between the aircraft and the surrounding atmosphere.

COUPLING. (11) The transfer of energy between wires or components of a circuit electrostatically, electromagnetically, or directly.

COVERAGE. (7) The percent confidence level of a given analytical redundancy fault detection and isolation algorithm for all types of faults.

COVERAGE. (9) The probability that when a fault occurs, it will be detected and recovery from the fault will be successful.

CRITICAL. (13) Functions whose failure would contribute to or cause a failure condition which would prevent the continued safe flight and landing of the aircraft.

CROSS COUPLING (CROSSTALK). (11) Transfer of signals from one channel, circuit, or conductor to another as an undesired or nuisance signal or the resulting noise.

DAMAGE. (11) The irreversible failure of a component.

DATA BUS. (6) A system for transferring data between discrete pieces of equipment in the same complex.

DATA LATENCY. (6) The delay from the time when a piece of information becomes available at a source terminal to the time it is received at the destination.

DATA LINK ASSURANCE OF RECEIPT. (6) The guarantee of good data through the data link level.

dB$\mu$V. (12) Decibels referred to one microvolt. Zero db represents one microvolt.

DECIBEL (dB). (11,12) Decibel expresses the ratio between two amounts of power, P1 and P2, at two separate points in a circuit. By definition, the number of dB = 10 log to the base 10 of (P1/P2). For special cases, when a standard power level P2 = 1 mW or 1 W or 1 kW, then the ratio is defined as "dBm," "dBw," or "dBKW." Because $P = V^2/R$ and also $I^2R$, decibels express voltage and current ratios. Ideally, the voltages and currents are measured at two points having identical impedances. By definition, dB = 20 log V1/V2 and dB = log I1/I2. For convenience, V2 or I2 are often chosen as 1 $\mu$V or 1 $\mu$A and the ratio is defined as dB above a $\mu$V or dB above a $\mu$A when graphing emission or susceptibility limits.

DECOUPLED MANEUVERS. (4) Changes in an aircraft's direction and attitude in one axis without affecting direction or attitude in other axes.

DESIGN ERROR. (4) A functional flaw resulting from a misinterpretation of the specifications of the system.

DESIGN MARGIN. (13) The difference between the equipment transient design levels and the transient control level.

DETERMINISTIC. (6) A system where all parameters are known, as opposed to a statistical system where the outcome is subject to the laws of probability.

DIAGNOSTIC FILTER. (7) An analytical algorithm which processes data from N functionally related sensors. The data are used to estimate some sensor outputs and assess the correct functioning of the sensors.

DIELECTRIC STRENGTH. (11) Voltage withstand capability that an insulating material sustains before destructive arcing and current flow, usually expressed in volts per mil thickness. Dielectric withstand voltage is the voltage level at which insulation breakdown occurs.

DIFFERENTIAL MODE (DM) SIGNAL. (11) The signal in a two-wire circuit measured from line-to-line.

DIRECT EFFECTS. (13) Any physical damage to the aircraft or onboard systems due to the direct attachment of the lightning channel. This includes tearing, bending, burning, vaporization, or blasting of aircraft surfaces or structures, and damage to electrical/electronic systems.

DISTRIBUTED CONTROL. (6) Concurrent control from multiple points in the data bus system.

DOUBLE FAIL-OPERATIONAL SYSTEM. (4) A quadruplex (or higher) redundant flight-control system which is designed to incur failures in two redundant lanes (or channels) before it fails.

DUAL FAIL-OPERATIONAL. (7) A reliability requirement placed on a system which requires the system to be operational after two failures have occurred.

DUAL GROUND. (11) Equipment case ground/return through two independent circuit paths to structure implemented in flammable zones and water leakage areas-each path meeting electrical conductivity (resistance) requirements.

DUAL-DUAL ARCHITECTURE. (4) Two parallel dual computers with a voting plane at the output of each dual computing lane.

ELECTRIC FIELD. (11) High-impedance, radiated voltage field, positive or negative, from a voltage source as contrasted to a low-impedance magnetic field from a current source.

ELECTROMAGNETIC COMPATIBILITY (EMC). (11) Operation within performance specification in the intended electromagnetic interference environment.

ELECTROMAGNETIC INTERFERENCE (EMI). (11) Conducted and radiated voltage/current noise signals, broadband (BB) or narrow band (NB), that degrade the specified performance of equipment.

ELECTROSTATIC CHARGE. (11) Electric potential energy with a surrounding electric field, uniform or nonuniform, moving or at rest, on a material.

EMISSION. (11) Voltage/current noise on a wire or in space. Broadband emission has uniform spectral energy over a wide frequency range and can be identified by the response of a measuring receiver not varying when tuned over several receiver "bandwidths." Or, energy present over a bandwidth greater than the resolution bandwidth where individual spectral components cannot be resolved. Broadband (BB) may be of two types: (1) impulse and coherent varies 20 dB per decade of bandwidth and (2) random or statistical, varies 10 dB per decade. A narrow band (NB) emission or signal, sometimes called continuous wave, occurs at a discrete frequency and does not vary with bandwidth.

ENVELOPE LIMITING. (4) General or additional limits imposed on the structural, "g" limits, speed, attitude, etc. of the aircraft. In some cases, envelope limiting imposes additional constraints on the envelope that cannot be exceeded regardless of pilot inputs.

EQUIPMENT TRANSIENT DESIGN LEVEL. (13) The level of transients which the equipment is qualified to withstand.

EQUIPMENT TRANSIENT SUSCEPTIBILITY LEVEL. (13) The transient level which will result in damage or upset to the system components. This level will be greater than the equipment transient design level.

ERROR. (4) A mistake in specification, design, production, maintenance, or operation of a system causing undesirable performance.

ERROR. (8) A state of the system which (in the absence of any corrective action by the system) could lead to a failure that would not be attributed to any event subsequent to the error. (More accurately known as an erroneous state.)

EVENT, EXTREMELY IMPROBABLE. (4) An event with a probability of occurrence on the order of $10^{-9}$ or less.

EVENT, IMPROBABLE. (4) An event with a probability of occurrence on the order of $10^{-5}$ or less.

EVENT, PROBABLE. (4) An event with a probability of occurrence on the order of $10^{-5}$ or greater.

EXTERNAL ENVIRONMENT. (13) Characterization of the natural lightning environment with idealized waveforms for engineering purposes.

FAILURE. (4) The inability of a system, subsystem, unit, or part to perform within specified limits.

FAILURE. (8) The situation when the external behavior of a system does not conform to that prescribed by the system specification.

FAILURE, HIDDEN. (4) A failure that is not manifested at the time of its occurrence.

FAIL-OPERATIONAL. (7) A reliability requirement placed on a system which requires the system to be operational after a single failure has occurred.

FAIL-SAFE. (7) A reliability requirement placed on a system which requires that safe flight not be hindered even after a failure.

FALL-TIME. (12) The time required for pulse amplitude to go from a predefined magnitude to a given level.

FALSE ALARM. (7) The declaration of a fault by a fault detection monitor or algorithm when there is no fault.

FAULT. (4) An error in the operation of a system.

FAULT. (8) The adjusted cause of error.

FAULT AVOIDANCE. (9) The attempt to prevent any software faults in the final delivered product through disciplined software development practices, testing, and IV&V.

FAULT CONTAINMENT. (6,9) The capacity of a system to prohibit errors and/or failures from propagating from the source throughout the system.

FAULT CURRENT. (11) The maximum current (magnitude and duration) flowing through a fault point. This current is equal to the supply voltage divided by the dc resistance of power line leads, circuit breakers, and the current return in wire or structure.

FAULT DETECTION. (6) The capacity of a system to determine the occurrence of erroneous operation.

FAULT DETECTION. (7) The determination that a sensor is faulted by using a software algorithm.

FAULT, HARD. (4) A defect in the hardware or software of a digital control system that permanently affects some functional performance of the system.

FAULT INSERTION. (4) A testing technique used to obtain information about data latency and built-in test coverage of a digital flight-control system.

FAULT ISOLATION. (6) The capacity of a system to isolate a failure to the required level so it can reconfigure.

FAULT ISOLATION. (7) The determination that a particular sensor is faulted by using a software algorithm.

FAULT, SOFT. (4) A transient defect in the software of a digital flight-control system that can be overcome by error-correctable code or by recycling of power to the computer system.

FAULT TOLERANCE. (6,9) The capability to endure errors and/or failures without causing total system failure.

FAULT TOLERANCE. (7) Accommodation of sensor hardware faults based on some type of comparator scheme.

FAULT TOLERANT. (4,9) Software which continues to operate satisfactorily in the presence of faults.

FAULT TREE ANALYSIS. (4) A top-down deductive analysis that identifies the conditions and functional failures necessary to cause a defined failure condition. The fault tree can be used to establish the probability of the ultimate failure condition occurring as a function of the estimated probabilities of contributory events.

FILTER. (11) Device or unit that passes or rejects a frequency band and is designed to block noise from entering or leaving a circuit or unit.

FLIGHT CODE. (4) The application software of the digital flight-control system.

FLIGHT-CRITICAL. (4,7) A description of functions whose failure would contribute to or cause a failure condition preventing the continued safe flight and landing of the aircraft.

FLIGHT-ESSENTIAL. (4) A description of functions whose failure would contribute to or cause a failure condition which would significantly affect the safety of the airplane or the ability of its crew to cope with adverse operating conditions.

FLIGHT-PHASE CRITICAL. (4) A description of functions which are critical only during certain phases of flight.

FLY-BY-GLASS. (16) Flight control system where fiber optics carry the signal.

FLY-BY-LIGHT. (4,16) Flight control system where fiber optics carry the signal.

FLY-BY-WIRE. (4,16) Flight control system with electric signaling.

FORWARD RECOVERY. (9) Restoration of the system to a consistent state by compensating for inconsistencies found in the current state so that the system may continue processing.

FOURIER TRANSFORM. (12) A mathematical method for deriving the frequency spectrum from a time dependent function.

GIGABIT. (16) One billion bits.

GLASS COCKPIT. (9) Advanced state-of-the-art electronic displays utilizing flat panel and/or cathode ray tube display technology for cockpit instrumentation.

GROUND EFFECT. (4) Increase in aircraft lift when operating near the ground.

GROUND. (11) A generic term having multiple meanings and indicating a circuit return path or a voltage reference: not "zero" voltage reference. Four hundred millivolts of noise voltage is common on "quiet" grounds. There are several types of returns and references.

HARD FAILURE. (12) A failure that requires a reset of the equipment.

HAZARD FUNCTION. (8) The conditional probability that a fault is exposed in the interval t to $\Delta t$ given that the fault did not occur prior to time t.

IMMUNITY. (11) Capability of a circuit or unit to operate within performance specification in a specified electromagnetic interference environment.

INDIRECT EFFECTS. (13) Voltage and/or current transients induced by lightning in aircraft electrical wiring which can produce upset and/or damage to components within electrical/electronic systems.

INDUCED VOLTAGES. (13) A voltage produced around a closed path or circuit by changing magnetic or electric fields or structural IR voltages.

INITIALIZATION. (6) Setting the beginning parameters and values on system power-up. For redundant systems this includes setting the initial configuration of the system.

INTERNAL ENVIRONMENT. (13) The fields and structural IR potentials produced by the external environment, along with the voltages and currents induced by them.

ISOLATION. (11) Electrical separation and insulation of circuits from ground and other circuits or arrangement of parts to provide protection and prevention of uncontrolled electrical contact.

JOULE. (12) A unit of energy equal to one watt-second.

JUMPER/STRAP. (11) A short wire, strip, strap, or braid conductor installed to make a safety ground connection, to dissipate electrostatic charge, or establish continuity around a break in a circuit.

KILOBYTE. (16) One thousand bytes.

LABELED ADDRESSING. (6) The system of identifying message recipients based on labels. This is in contrast to destination terminal addresses.

LATENT FAULT. (10) A fault which has not yet produced a malfunction. (In the context of the single-fault model, benign and latent faults are equivalent.)

LIGHTNING FLASH. (13) The total lightning event in which charge is transferred from one charge center to another. It may occur within a cloud, between clouds, or between a cloud and the ground. It can consist of one or more strokes, plus intermediate or continuing currents.

LIGHTNING LEADER STROKE. (13) The leader forms an ionized path for charge to be channeled towards the opposite charge center. The stepped leader travels in a series of short, luminous steps prior to the first return stroke. The dart leader reionizes the return stroke path in one luminous step prior to each subsequent return stroke in the lightning strike.

LIGHTNING RETURN STROKE. (13) A lightning current surge that occurs when the lightning leader makes contact with the ground or an opposite charge center.

LIGHTNING STRIKE. (13) Any attachment of the lightning flash to the aircraft.

LIGHTNING STRIKE ZONES. (13) Locations on the aircraft where the lightning flash will attach or where substantial amounts of electrical current may be conducted between attachment points. The location of these zones on any aircraft is dependent on the aircraft's geometry and operational factors and often varies from one aircraft to another.

LIMITING, VOLTAGE/CURRENT. (11) Semiconductor components, diodes, Transorb, or filter designed to clip and shunt to ground an applied transient or steady-state voltage. Used to protect against noise frequencies, faults, lightning, and inductive switching transients.

LOW-PASS FILTER. (12) An electrical circuit which allows the passage of low frequencies and prevents the passage of high frequencies.

MAGNETIC FIELD. (11) A radiated, low-impedance field having lines of "flux" or magnetomotive force associated with an electrical current.

MALFUNCTION. (11) Failure or degradation in performance that compromises flight safety.

MEAN AERODYNAMIC CHORD (also mean chord). (4) The chord of an airfoil whose length is equal to the area of the airfoil section divided by the span.

MEAN FAILURE RATE. (10) A measure of survivability defined as the reciprocal of the mean time to system failure.

MESSAGE STRUCTURE. (6) The organization of both protocol and data information in a message.

MICRON. (16) One-millionth of a meter.

MISSED ALARM. (7) The failure of a fault detection monitor or algorithm to detect a fault when there is a sensor fault.

MONITORABILITY. (6) The capacity of the protocol to be viewed passively to allow observation of the dynamics of the protocol.

MULTIPLE BURST. (13) A randomly spaced series of bursts of short duration, low amplitude current pulses, with each pulse characterized by rapidly changing currents. These bursts may result from lightning leader progression or branching and may be accompanied by or superimposed on stroke or continuing currents. The multiple bursts appear to be most intense at the time of initial leader attachment to the aircraft.

MULTIPLE STRIKE. (13) Two or more lightning strikes during a single flight.

MULTIPLE STROKE. (13) Two or more return strokes occurring during a single lightning flash.

MULTIPLE TRIP MONITOR. (7) A fault detection algorithm which declares a fault after the sensor output has exceeded a predefined threshold N times.

NANOSECOND. (16) One-billionth of a second.

NEGATIVELY STABILIZED. (4) Aircraft design in which the point of effective lift is aft of the center of gravity.

NETWORK CONTROL STRATEGY. (6) The solution proposed by the designer in addressing his specific problem (design flexibility).

NOISE. (11) Conducted or radiated emission causing circuit upset, performance disorder, or undesired sound.

NUMERICAL APERTURE. (6) The angle of acceptance of light from a light source for a given fiber optic cable.

OBSERVER. (7) An algorithm which models physical relationships between sensor data and uses the data to provide fault detection for one or more sensors. This is also known as a Luenberger observer or a signal blender.

PARAMETERIZATION CAPABILITY. (6) A measure of how well the attributes of the protocol can be described by parameters.

PEAK RATE OF RISE. (13) The maximum instantaneous slope of the waveform as it rises to its maximum value. Mathematically, the peak rate of rise of a function, i(t), may be expressed as the maximum of d[i(t)]/dt.

PIN LEVEL TEST. (12) An EMC test in which voltage or current is applied directly to a conductor at a connector pin.

POINT-MASS SIMULATION. (4) Same as state variables airplane model (q.v.)

POSITIVELY STABILIZED AIRCRAFT. (4) Aircraft design in which the effective point of lift is forward of the center of gravity.

PRECIPITATION STATIC (P-static). (11) Electrostatic discharge, corona, arcing, and streamering, steady state or impulsive, causing circuit upset, receiver noise or component damage.

PREDICATE/TRANSITION NETWORK. (4) A bipartite graph (a type of linear graph) to model concurrency between redundant concurrent events. Basically a modified generalized petri net.

Q. (12) The quality factor of a resonant circuit which is the ratio of the energy stored to the power dissipated per cycle.

QUADRUPLEX ARCHITECTURE. (4) The use of four separate lanes (or channels) of computer redundancy. Each lane can fail separately providing a fail-operational capability for the digital flight-control system.

RADIATED EMISSION (RE). (11) Electromagnetic energy transmitted and propagated in space usually considered as audio frequency or radio frequency noise.

RADIO FREQUENCY (RF). (11) Frequencies in the electromagnetic spectrum used for radio communications extending from kilohertz to gigahertz.

RADIO FREQUENCY INTERFERENCE (RFI). (11) Electromagnetic interference in the radio frequency range.

RECONFIGURATION. (6) The capacity of a system to rearrange or reconnect the system elements or functions.

RECOVERY CACHE. (9) The location used to preserve input values until the outputs resulting from them have been accepted.

REDUNDANCY MANAGEMENT. (7) The computer processing which is needed to implement fault detection and isolation algorithms.

REFERENCE. (11) 1. Structure, for electronics, shields, power. 2. A grid of wires, solid sheet, or foil. 3. A wire from circuit to grounding block or case. 4. A wire from circuit to structure. 5. Shield tie. 6. Earth.

RELAXED STATIC STABILITY AIRCRAFT. (4) An aircraft whose center of gravity is behind the wing's point of effective lift.

RELIABILITY ANALYSIS. (4) A means of determining the probability of failure in a system. Military flight-critical systems typically are required to have reliability levels of $10^{-5}$ to $10^{-7}$, whereas civil flight-critical systems have reliability levels of $10^{-9}$ or less.

RESONANCE. (12) Resonance occurs in an electrical circuit when the energy stored in the inductance is equal to the energy stored in the capacitance.

RETURN STROKE. (13) See lightning return stroke.

RETURN. (11) 1. Structure, for power, fault, and "discrete" circuits. 2. A grid of wires, solid sheet, or foil. 3. A wire from circuit load back to source or to case. 4. Circuit card "ground plane," also a reference and shield.

REVERSION MODE. (7) The high level of redundancy in a system having different redundancy requirements for some sensors. Critical sensors may have a high level of redundancy while other sensors have low levels.

RISE-TIME. (12) The time required for a voltage pulse to reach a predefined magnitude from a given level.

ROBUSTNESS. (9) The ability of the code to perform despite some violation of the assumptions in its specifications usually via substitution of an alternate value and continuation of execution if a software fault is detected.

ROLLBACK. (9) Retrying the calculation in the event that a failure is detected, under the assumption that some external condition may have changed thereby resolving the anomaly.

SEALANT. (11) An applied substance enclosing and protecting the integrity of a joint, fastener, or electrical bond from moisture, contaminants, oxidation, and acid or alkaline corrosion.

SENSOR. (7) An instrument which measures a particular physical parameter. The data output may be digital or analog and is utilized by the flight computer.

SEQUENTIAL LIKELIHOOD RATIO TEST. (7) A fault detection algorithm which is based on two hypothesized density functions of no fault or sensor fault.

SEQUENTIAL PROBABILITY RATIO TEST. (7) See sequential likelihood ratio test.

SHIELD. (11) A conductive material, opaque to electromagnetic energy, for confining or repelling electromagnetic fields. A structure, skin panel, case, cover, liner, foil, coating, braid, or cable-way that reduces electric and magnetic fields into or out of circuits or prevents accidental contact with hazardous voltages.

SHIELD EFFECTIVENESS (SE). (11) The ability of a shield to reject electromagnetic fields. A measure of attenuation in field strength at a point in space caused by the insertion of a shield between the source and the point.

SHIELDING. (12) Any metallic structure such as the aircraft fuselage or the woven braid on a cable that provides protection against electromagnetic fields.

SIGNAL RETURN. (11) A wire conductor between a load and the signal or driving source. Structure can be a signal and power return. Commonly, it is the low voltage side of the closed loop energy transfer circuit.

SINGLE-ENDED CIRCUIT. (11) A circuit with source and load ends grounded to case and structure and using structure as return.

SINUSOID. (12) A wave form that follows the mathematical values of a sine function.

SOFT FAILURE. (12) A failure which causes an alteration of data or missing data.

STATE-VARIABLE AIRPLANE MODEL (also point-mass model). (4) Fixed aerodynamic variables are used in the solution of the equations of motion of the model instead of using look-up tables in which each derivative varies with airspeed, altitude, etc. The model performance is only accurate at or near the point in the flight envelope for which the variables are chosen.

STATIC MARGIN. (4) The degree of instability in a relaxed statically stable airplane.

STRUCTURAL IR VOLTAGE. (13) The portion of the induced voltage resulting from the product of the distributed lightning current, I, flowing through the resistance, R, of the aircraft skin or structure.

STRUCTURE. (11) Basic members, supports, spars, stanchions, housing, skin panels, or coverings that may or may not provide conductive return paths and shields for electrical/electronic circuits.

SUPER-DIAGNOSTIC FILTER. (7) An algorithm which provides all the capabilities of a diagnostic filter. Additionally, it can isolate a specific faulted sensor. At the current time, this is the most complex technique used to implement analytical redundancy.

SUSCEPTIBILITY. (11) Upset behavior or characteristic response of an equipment when subjected to specified electromagnetic energy. Identified with the point, threshold, or onset of operation outside of performance limits. Conducted Susceptibility (CS) applies to energy on interface conductors; Radiated Susceptibility (RS) to radiated fields.

SWEPT STROKE. (13) A series of successive attachments due to sweeping of the flash across the surface of the airplane by the motion of the airplane.

SYNCHRONOUS MESSAGES. (6) Messages transmitted at a known a priori sequence and time or time interval.

SYSTEM EXPOSURE TIME. (4) The period during which a system may fail. This period extends from the last verified proper functioning to the completion of the next required performance.

SYSTEM FUNCTIONAL UPSET. (13) Impairment of system operation, whether permanent or momentary (e.g., a change of digital or analog state) which may or may not require manual reset.

SYSTEM INTEGRITY. (6) The degree to which a system is dependable.

TESTABILITY. (6) A measure of how well the protocol supports completeness of testing and the protocol's ability to produce repeatable or predictable results.

THRESHOLD, NOISE. (11) The lowest electromagnetic interference signal level that produces onset of susceptibility.

THROUGHPUT. (6) The productivity of a data processing system as expressed in computing work per minute or hour.

THYRISTORS. (16) Solid-state devices that convert alternating current to direct current.

TIME CONSTANT. (4) Time required to double the amplitude of the divergent real root in the pitch axis of the aircraft model.

TRANSIENT CONTROL LEVEL. (13) The maximum allowable level of transients appearing at the systems interfaces as a result of the defined external environment.

TRANSPARENT RECOVERY. (4) Correcting a soft fault without interrupting the system's intended performance.

TRIBOELECTRIC CHARGING. (13) Static electricity produced on a structure from the effects of friction.

UNACCEPTABLE RESPONSE. (11) Upset, degradation of performance, or failure, not designated a malfunction, but is detrimental or compromising to cost, schedule, comfort, or workload.

UNDESIRABLE RESPONSE. (11) Change of performance and output, not designated a malfunction or safety hazard, that is evaluated as acceptable as is because of minimum nuisance effects and excessive cost burdens to correct.

UPSET. (11) Temporary interruption of performance that is self-correcting or reversible by manual or automatic process.

UPSET. (12) A condition in which the state of a digital device is unintentionally altered, but may be restored by automatic means or by operator intervention.

UPSET. (13) See system functional upset.

VALIDATION. (4,11) Demonstration and authentication that a final product operates in all modes and performs consistently and successfully under all actual operational and environmental conditions founded upon conformance to the applicable specifications.

VERIFICATION. (4,11) Demonstration by similarity, previous in-service experience, analysis, measurement, or operation that the performance, characteristics, or parameters of equipment and parts demonstrate accuracy, show the quality of being repeatable, and meet or are acceptable under applicable specifications.

VOTING PROCEDURE. (8) An algorithm included in fault tolerant software which uses the consensus recovery block method. It compares outputs of the n independent versions and determines which outputs are correct by identifying agreements among two or more versions.

## ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| μm (6) | Micrometer |
| φM (6) | Phase Modulation |
| 3-D (16) | Three-Dimensional |
| ac (3,6,12) | Alternating Current |
| AC (3,14) | Advisory Circular |
| A/C (11) | Aircraft |
| ACAP (13) | Advanced Composite Airframe Program |
| ACARS (11,12) | ARC Communications Addressing and Reporting System |
| ACES (13) | Applied Computational Electromagnetics Society |
| ACS (16) | Automatic Control System |
| ACT (11,12) | Active Controls Technology |
| ADC (11,12) | Air Data Computer |
| ADF (11,12) | Automatic Direction Finder |
| ADI (3) | Automatic Direction Indicator |
| AE (6) | Avionics Equipment |
| AE4L (13) | SAE Subcommittee (Lightning) |
| AEHP (13) | Atmospheric Electricity Hazards Protection |
| AERA (16) | Automated En Route Air Traffic Control System |
| AES-S (6) | Aerospace and Electronic Systems Society |
| AF (11,12) | Audio Frequency |
| AFBW (4) | Augmented Fly-By-Wire |
| AFCS (11,12) | Automatic Flight Control System |
| AFFDL (7,8,13) | Air Force Flight Dynamics Laboratory |
| AFM (16) | Advanced Fuel Management |
| AFWAL (6,13) | Air Force Wright Aeronautical Laboratory |
| AGARD (8) | Advisory Group for Aerospace Research and Development |
| AHRS (6) | Attitude Heading Reference System |
| AI (16) | Artificial Intelligence |
| AIAA (6,9) | American Institute for Aeronautics and Astronautics |
| AK (7) | Altitude Kinematics |
| A/L (3) | Approach/Land |
| ALCM (13) | Air Launched Cruise Missile |
| ALU (3,10) | Arithmetic Logic Unit |
| AM (6,14) | Amplitude Modulation |
| ANSI (11,12) | American National Standards Institute |
| AOA (4) | Angle of Attack |
| APU (11,12) | Auxiliary Power Unit |
| AR (7) | Analytical Redundancy |
| ARC (11,12) | Aeronautical Radio, Incorporated |
| ARIES (3) | Automated Reliability Interactive Estimation System |
| ARINC (3,6) | Aeronautical Radio, Incorporated |
| ASCB (6) | Avionics Standard Communications Bus |
| ASDS (11,12) | Airport Surface Detection System |
| ATCRBS (11,12,14) | Air Traffic Control Radar Beacon System |

| | |
|---|---|
| ATF (16) | Advanced Tactical Fighter |
| ATI (16) | Access Time Interval |
| AWACS (14) | Airborne Warning and Control System |
| BB (11,12) | Broadband |
| BCI (12) | Bulk Cable Injection |
| B-dot (13) | Derivative of the magnetic field with respect to time |
| BGU (10) | Bus Guardian Unit |
| BIR (6) | Benchmark Information Rate |
| BIT (6) | Built-In Test |
| BITE (6,11,12) | Built-In Test Equipment |
| BIU (6) | Bus Interface Unit |
| bps (6) | Bits Per Second |
| BW (11,12) | Bandwidth |
| C (7) | Comparator |
| CAA (14) | Civil Aviation Authority |
| CAPS (3) | Computer Aided Production Simulator |
| CARE (3) | Computer Aided Reliability Evaluator |
| CARSRA (3,7) | Computer-Aided Redundant System Reliability Analysis |
| CAS (11,12) | Criticality Advisory System |
| CAST (3) | Complementary Analytic Simulative Technique |
| CCITT (6) | Consultative Committee for International Telephone and Telegraph |
| CD (6) | Collision Detection |
| cdf (8) | Cumulative Density Function |
| CDU (11,12) | Control Display Unit |
| CE (11,12) | Conducted Emission |
| CM (11,12) | Common Mode |
| CMOS (12) | Complimentary Metal-Oxide Semiconductor |
| CONUS (14) | Contiguous United States |
| CPU (10) | Central Processing Unit |
| CR (6) | Command Response |
| CRC (6) | Cyclic Redundancy Check |
| CRMI (2) | Computer Resource Management, Incorporated |
| CRT (11,12,16) | Cathode Ray Tube |
| CS (11,12) | Conducted Susceptibility |
| CSC (9) | Computer Software Component |
| CSCI (9) | Computer Software Configuration Item |
| CSDL (10) | Charles Stark Draper Laboratories |
| CSMA (6,16) | Carrier Sensed Multiple Access |
| CSMA/CD (6) | Carrier Sense Multiple Access/Collision Detection |
| CT (2,6) | Technical Center (designation used in FAA report numbering scheme) |
| CTA (3) | CAPS Test Adapter |
| CW (13) | Continuous Wave |
| DADC (6) | Digital Air Data Computer |
| DARPA (16) | Defense Advanced Research Projects Agency |
| DATAC (6) | Digital Autonomous Terminal Access Communication |
| dB (6,12) | Decibel |
| dBi (14) | Decibels with respect to one milliampere |

| | |
|---|---|
| dBm (6) | Decibels per meter |
| dc (6,12) | Direct Current |
| DF (7) | Diagnostic Filter |
| DFC (7) | Digital Flight Control |
| DFCS (3,4,7,16) | Digital Flight Control System |
| DFDAU (11,12) | Digital Flight Data Acquisition Unit |
| DFDR (11.12) | Digital Flight Data Recorder |
| DGAC (14) | Directorate Generale Aviation Civile |
| DITS (6,11,12) | Digital Information Transfer System |
| DM (6) | Delay Modulation |
| DM (11) | Differential Mode |
| DMA (6) | Direct Memory Access |
| DME (11,12) | Distance Measuring Equipment |
| DNA (13) | Defense Nuclear Agency |
| DOD (8,12,14,16) | Department of Defense |
| DOE (13) | Department of Energy |
| DOT (2,3,6,7,8) | Department of Transportation |
| DRB (9) | Distributed Recovery Block |
| DSP (3) | Discrete Switch Panel |
| | |
| E (11,12) | Electromagnetic Environmental Effects |
| EADI (11,12) | Electronic Attitude Director Indicator |
| ECAC (11,12,14) | Electromagnetic Compatibility Analysis Center |
| ECM (14) | Electronic Counter Measures |
| ECS (11,12) | Environmental Control System |
| E-dot (13) | Derivative of the electric field with respect to time |
| E/E (11,12) | Electrical/Electronic |
| EEC (11,12) | Electronic Engine Control |
| EED (11,12) | Electro-Explosive Device |
| E-FIELD (11,12) | Electric Field |
| EFIS (11,12) | Electronic Flight Instrument System |
| EFMA (3) | Executive Failure My A |
| EFMB (3) | Executive Failure My B |
| EFOA (3) | Executive Failure Other A |
| EFOB (3) | Executive Failure Other B |
| EFW (3) | Executive Failure Word |
| EGT (11,12) | Exhaust Gas Temperature |
| EHSI (11,12) | Electronic Horizontal Situation Indicator |
| EICAS (11,12) | Engine Indication and Crew Alerting System |
| EIU (16) | Electronic Interface Unit |
| EM (11,12,13) | Electromagnetic |
| EMAS (2) | Electromechanical Actuator System |
| EMC (6,11,12,13,14) | Electromagnetic Compatibility |
| EMCad$^{tm}$ (12) | Electromagnetic Computer aided design |
| EME (11,12) | Electromagnetic Effects |
| EME (14) | Electromagnetic Environment |
| EMI (6,11,12,13,16) | Electromagnetic Interference |
| EMIC (11,12) | Electromagnetic Interference/Compatibility |
| EMP (11,12,13) | Electromagnetic Pulse |
| EMR (14) | Electromagnetic Radiation |
| EMUX (6) | Electrical Multiplex |
| ENRZ (6) | Enhanced Non-return to Zero |

| | |
|---|---|
| EPR (11,12) | Engine Pressure Ratio |
| EPROM (16) | Erasable Programmable Read-Only Memory |
| ESD (11,12) | Electrostatic Discharge |
| ESE (11,12) | Electric (field) Shield Effectiveness |
| ESS (9) | Electronic Switching System |
| ETDL (13) | Equipment Transient Design Level |
| EUROCAE (14) | European Organization for Civil Aviation Electronics |
| FAA (ALL) | Federal Aviation Administration |
| FADEC (6,16) | Full Authority Digital Engine Controller |
| FAFTEEC (16) | Full Authority Fault Tolerant Electronic Engine Control |
| FAR (3,4,6,16) | Federal Acquisition Regulation |
| FBL (16) | Fly-By-Light |
| FBW (4,7,16) | Fly-By-Wire |
| FCC (3,4,6,10,11,12) | Flight Control Computer |
| FCS (4,10,16) | Flight Control System |
| FD (7) | Fault Detection |
| FDEP (11,12) | Flight Data Entry Panel |
| FET (16) | Field Effect Transistor |
| FI (7) | Fault Isolation |
| FIIS (10) | Fault Insertion and Instrumentation System |
| FM (6,14) | Frequency Modulation |
| FMC (11,12) | Flight Management Computer |
| FMEA (3,9) | Failure Mode and Effect Analysis |
| ft (14) | feet |
| FTMP (10) | Fault-Tolerant Multiprocessor |
| GaAs (6,16) | Gallium Arsenide |
| GAMA (6) | General Aviation Manufacturers' Association |
| GCR (6) | Group Code Recording |
| G/E (13) | Graphite Epoxy |
| GEMACS (13) | General Electromagnetic Model for the Analysis of Complex Systems |
| GNC (16) | Guidance, Navigation, and Control |
| GPS (11,12) | Global-Positioning-System |
| GPWS (11,12) | Ground Proximity Warning System |
| Gr/Ep (11,12) | Graphite/Epoxy |
| GS (10) | Glideslope |
| H1 (11,12) | Fan Speed |
| HDLC (6) | High-Level Data Link Control |
| HERF (14,16) | High-Energy Radio Frequency |
| HF (11,12,13,14) | High-Frequency |
| H-FIELD (11,12) | Magnetic Field |
| HSI (3) | Horizontal Situation Indicator |
| HSRB (6) | High-Speed Ring Bus |
| Hz (3) | Hertz |
| I (13) | Current |
| IAA (3) | Integrated Assurance Assessment |
| IAAC (11,12) | Integrated Application of Active Controls Technology (to an Advanced Subsonic Transport Project) |

| | |
|---|---|
| IC (3) | Integrated Circuit |
| ICAO (14) | International Civil Aviation Organization |
| IDG (11,12) | Integrated Drive Generator |
| I-dot (13) | Derivative of the current with respect to time |
| IEEE (6,9) | The Institute for Electrical and Electronics Engineers, Incorporated |
| IFF (14) | Identification - Friend or Foe |
| ILS (3,11,12) | Instrument Landing System |
| INS (6,11,12) | Inertial Navigation System |
| I/O (10) | Input/Output |
| IRS (11,12) | Inertial Reference System |
| ITT (16) | (Consultative Committee for) International Telegraphy and Telephony |
| IV&V (9) | Independent Verification and Validation |
| K (6) | Thousand |
| kA (13,16) | Kiloampere |
| kHz (6,12,14) | Kilohertz |
| km (6) | kilometer |
| LCC (11,12) | Life Cycle Cost |
| LCD (16) | Liquid Crystal Display |
| LED (6) | Light Emitting Diode |
| LF (13) | Low Frequency |
| LOC (11,12) | Localizer |
| LPN (13) | Lumped Parameter Network |
| LRC (6) | Longitudinal Redundancy Check |
| LRRA (11,12) | Low Range Radio Altimeter |
| LRU (6,11,12,13) | Line Replaceable Unit |
| LSB (6) | Least Significant Bit |
| LTPB (6) | Linear Token Passing Bus. |
| LTRI (13) | Lightning and Transients Research Institute |
| LVDT (3) | Linear Voltage Differential Transducer |
| M (6) | Million |
| m (6) | meter |
| mA (3) | Milliampere |
| MAADS (6) | Multibus Avionic Architecture Design Study |
| MAC (4) | Mean Aerodynamic Chord |
| MAFT (16) | Multicomputer Architecture for Fault Tolerance |
| Mbps (6,16) | Million bytes per second |
| MCDP (11,12) | Maintenance Control and Display Panel |
| MCP (11,12) | Mode Control Panel |
| MDICU (3) | Modular Digital Interface Control Unit |
| MDICU (4) | Modular Digital Interface Conversion Unit |
| MDT (6) | Mean Down Time |
| Mflops (16) | Million floating-point operations per second |
| MFM (6) | Modified-Frequency Modulation |
| MFR (10) | Mean Failure Rate |
| MHz (6,12,14) | Megahertz |
| mil (11,12) | One thousandths of an inch (0.001) |
| MIL-STD (6) | Military Standard |

| | |
|---|---|
| MLE (8) | Maximum Likelihood Estimates |
| MLS (11,12) | Microwave Landing System |
| MPP (16) | Massively Parallel Processor |
| ms (6,10) | Millisecond |
| MSB (6) | Most Significant Bit |
| MSE (11,12) | Magnetic (Field) Shielding Effectiveness |
| MTBCF (6) | Mean Time Between Critical Failures |
| MTBF (9) | Mean Time Between Failures |
| MTTF (8,10) | Mean Time to Failure |
| MTTR (6) | Mean Time To Repair |
| MUX (4) | Multiplexer |
| N2 (11,12) | Core Engine Speed |
| NA (3) | Normal Accelerometers |
| NA (6) | Numerical Acceptance |
| NADC (6,7) | Naval Air Development Center |
| NAECON (6) | National Aerospace & Electronics Conference |
| NASA (2,3,7,13) | National Aeronautics and Space Administration |
| NASC (13) | Naval Air Systems Command |
| NATO (14) | North Atlantic Treaty Organization |
| NB (11,12) | Narrow Band Signal |
| NEC (13) | Numerical Electromagnetics Code |
| NEMP (12) | Nuclear Electromagnetic Pulse |
| NHPP (8) | Non-Homogeneous Poisson Process |
| nmi (14) | nautical mile |
| NPRM (14) | Notice of Proposed Rulemaking |
| NRZ (6) | Non-return to Zero |
| NRZ-I (6) | Non-return to Zero Inverted |
| NRZ-L (6) | Non-return to Zero Dual Level |
| nsec (6) | Nanosecond |
| NSWC (13) | Naval Surface Weapons Center |
| NVS (8) | N-version Software |
| OMEGA (11,12) | Very Low Frequency Navigation |
| OMV (16) | Orbital Maneuvering Vehicle |
| OTV (16) | Orbital Transfer Vehicle |
| P (10) | Processor |
| PAS (6) | Pilot Assist System |
| PCS (16) | Primary Control System |
| PCU (11,12) | Power Control Unit |
| pdf (8) | Probability Density Function |
| PE (6) | Phase Encoding |
| pf (12) | picofarad |
| PLA (16) | Power Level Angle |
| PRF (11,12) | Pulse Repetition Frequency |
| PROM (3,10) | Programmable Read-Only Memory |
| P-Static (11,12) | Precipitation Static |
| PVI (16) | Pilot/Vehicle Interface |
| PWM (11,12) | Pulse Width Modulation |

| | |
|---|---|
| R (13) | Resistance |
| RADC (8) | Rome Air Development Center |
| RAE (13) | Royal Aircraft Establishment |
| RAM (3,10,16) | Random Access Memory |
| RAT (6) | Ring Admittance Timer |
| RB (8) | Recovery Block |
| RBDCP (3) | Reliability Block Diagram Computer Program |
| R-C (12) | Resistor-Capacitor |
| RCA (16) | Radio Corporation of America |
| RDFCS (3) | Redundant Digital Flight Control System |
| RDFCS (4) | Reconfigurable Digital Flight Control System (facility) |
| RDMI (11,12) | Radio Distance Magnetic Indicator |
| RE (11,12) | Radiated Emission |
| REL (3) | Reliability |
| REL COMP (3) | Reliability Computers |
| RF (11,12,13,14,16) | Radio Frequency |
| RFI (11,12) | Radio Frequency Interference |
| RL (13) | Resistance/Inductance |
| RLC (13) | Resistance/Inductance/Capacitance |
| RLCM (13) | Resistance/Inductance/Capacitance/Mutual |
| RM (7) | Redundancy Management |
| RNRZ (6) | Randomized Non-return to Zero |
| ROM (10) | Read Only Memory |
| RPV (16) | Remotely Piloted Vehicle |
| RS (11,12) | Radiated Susceptibility |
| RSS (4,7) | Relaxed Static Stability |
| RTCA (2,3,11,12,14,16) | Radio Technical Commission for Aeronautics |
| RZ (6) | Return to Zero |
| | |
| S/A (11,12) | Spectrum Analyzer |
| S-a-0 (10) | Stuck at Zero |
| S-a-1 (10) | Stuck at One |
| SAE (2,6,13,14,16) | Society of Automotive Engineers |
| SAS (4,7) | Stability Augmentation System |
| SDF (7) | Super-Diagnostic Filter |
| SE (11,12) | Shielding Effectiveness |
| SHF (11,12) | Super High-Frequency |
| SIF (14) | Selective Identification Facility |
| SLRT (7) | Sequential Likelihood Ratio Test |
| SMOTEC (14) | Special Missions Operation Test and Evaluation Center |
| SPRT (7) | Sequential Probability Ratio Test |
| SSP (3) | Servo Simulation Panel |
| STANAG (14) | Standardization Agreement (NATO) |
| STC (2) | Supplemental Type Certification |
| STOL (16) | Short Takeoff and Landing |
| str (6) | string |
| | |
| TACAN (14) | Tactical Air Navigation |
| TASRA (3) | Tree Aided System Reliability Analysis |
| TC (2) | Type Certification |
| TCAP (13) | Threshold Circuit Analysis Program |
| TCAS (11,12,16) | Traffic Alert and Collision Avoidance System |

| | |
|---|---|
| TCL (13) | Transient Control Level |
| TDM (6) | Time Division Multiplex |
| THT (6) | Token-Holding Timer |
| TLA (11,12) | Thrust Lever Angle |
| TMC (11,12) | Thrust Management Computer |
| TMR (10) | Triple Modular Redundant |
| T/R (6) | Transmitter/Receiver |
| TTL (11,12,13,16) | Transistor-Transistor Logic |
| TV (14) | Television |
| TWTD (13) | Thin Wire Time Domain |
| UHF (11,12,13,14) | Ultra High-Frequency |
| U.K. (13,14) | United Kingdom |
| U.S. (14) | United States |
| USAF (16) | United States Air Force |
| USB (16) | Upper Surface Blowing |
| VHF (11,12,13,14) | Very High-Frequency |
| VHSIC (6,16) | Very-High-Speed Integrated Circuits |
| VLF (11,12) | Very Low-Frequency |
| VLSI (6,14) | Very Large Scale Integration |
| VLSIC (6,16) | Very Large Scale Integrated Circuits |
| V/m (14) | Volt/meter |
| VOR (11,12,14) | VHF Omnidirectional Range |
| VORTA/VHF (11,12) | Omnirange/Tactical Air Navigation |
| VRC (6) | Vertical Redundancy Check |
| VSI (11,12) | Vertical Speed Indicator |
| VTOL (16) | Vertical Takeoff and Landing |
| WAI (3) | Warning Annunciation Indicator |
| WRU (11,12) | Weapons Replaceable Unit |
| XMTR (3) | Transmitter |
| ZM (6) | Zero Modulation |

# SUPPLEMENTARY

# INFORMATION

ERRATA

# ERRATA

Report No. DOT/FAA/CT-88/10

DIGITAL SYSTEMS VALIDATION HANDBOOK - VOLUME II

February 1989

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NJ 08405

Replace the following pages in Chapter 10:

10-13, 10-14, 10-15, 10-16, 10-17, 10-18, 10-19, 10-20

Released October 1989

(Henceforth, we will assume that there is only a single auxiliary program. If more than one auxiliary program were involved, the complexity of the model would increase.)

The parameters of the model are not independent. In fact,

$$p_1 + p_2 + p_3 = 1$$

$$p_2 = (1 - p_1)\left[ \frac{as}{as + ds} \right]$$

$$p_3 = (1 - p_1)\left[ \frac{ds}{as + ds} \right]$$

From the results of the FIIS and previous experiments it was expected to obtain estimates of $p_1$, $p_3$, $e_\alpha$, and $e_\beta$. The parameters $p_2$, as, and ds would be obtained from typical FCS scenarios (e.g., duration of and time between initiation of auxiliary programs).

### 3.2. Parameter Estimates

- $p_1$: From the Bendix study, $.85 < p_1$; from FIIS, $.96 < p_1 < .98$
- $p_2$: It is estimated that $p_2 = 0$, approximately
  (With $p_2 = 0$, $1 - p_1$ = proportion of latent faults)
- $p_3$: From the Bendix study, $p_3 < .15$; from FIIS, $.02 < p_3 < .04$
- $e_\alpha$: From the FIIS study, $e_\alpha > 7200$/hour
- $e_\beta$: From the FIIS study, $e_\beta > 900$/hour
- as: From FCS scenarios, .01/hour < as < 10/hour
- 1/ds: From FCS scenarios, .01 hours < 1/ds < 1 hour
- f: The current range is .001/hour < f < .0001/hour

### 3.3. Potential Criticality of Latent Faults

In order to assess the effects of latent faults, we present two examples of conventional FCSs which could be vulnerable to the accumulation of latent faults. The examples noted are Triplex FCS (section 3.4) and Quadruplex FCS (section 3.5). The scenario is one in which latent faults, when activated, lead to a rapid and unexpected loss of components. Such a condition can arise in a Quadruplex FCS, where for example, in time, three out of the four lanes develop latent faults. Eventually, due to a single source of excitation, such as the callup of an outer-loop program, the faults become active. Even assuming, as we do, that the time interval between the successive activation of the faults (referred to, hereafter, as "avalanching latent faults") is sufficient to allow the comparators to detect and isolate each fault in turn, the result is a loss of the three lanes in quick succession. It is our contention that the probability of such an event may not be insignificant.

### 3.4. Example 1 - Triplex FCS

The conventional reliability analysis, which assumes that there are no faults at the start of each flight, would conclude that the probability of loss of the FCS function in a flight of one hour is $3f^2$.

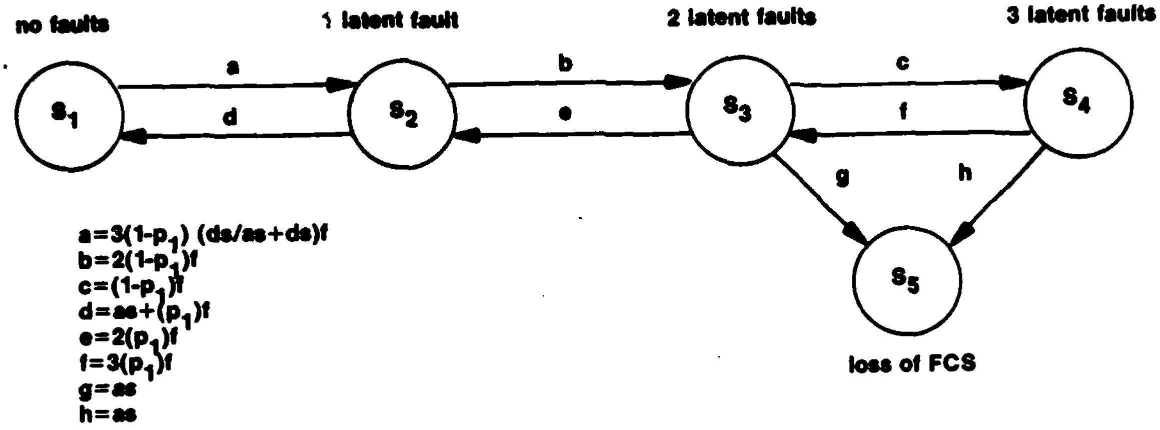


FIGURE 3.4-1. MARKOV MODEL/TRIPLEX FCS WITH LATENT FAULTS

A Markov reliability model of the FCS, representing the effects of avalanching latent faults, is shown in figure 3.4-1. The following assumptions are implicit:

- Loss of control is due, exclusively, to avalanching latent faults.
- Faults are exponentially distributed.
- The time between the successive activation of multiple latent faults is small relative to mission time.
- $\alpha$-faults (i.e., faults active at their occurrence) are detected immediately as they occur, at which time the entire lane is replaced. Thus, existing latent faults are effectively repaired.

- Excitation of latent faults is assumed to be correlated across lanes (i.e., a single excitation activates latent faults in different lanes).

Referring to figure 3.4-1:

- State $S_1$ represents the condition that all lanes are fault-free.
- State $S_2$ has a latent fault in one lane.
- State $S_3$ has a latent fault in two lanes.
- State $S_4$ has a latent fault in three lanes.
- State $S_5$ represents loss of the FCS function.

The transition rates are:

$$a = 3(1-p_1)f[\frac{ds}{as + ds}]$$

$$b = 2(1-p_1)f$$

$$c = (1-p_1)f$$

$$d = as + (p_1)f$$

$$e = 2(p_1)f$$

$$f = 3(p_1)f$$

$$g = as$$

$$h = as$$

It is noted that the backward transitions (d, e, and f) are the result of repairs due to the detection of $\alpha$-faults.

Let $x_1$, $x_2$, $x_3$, $x_4$, and $x_5$ denote the occupancy probabilities of states $S_1$, $S_2$, $S_3$, $S_4$, and $S_5$, respectively. From the figure we obtain the following differential equations:

$$\begin{aligned}
sX_1 - x_1(0) &= -aX_1 + dX_2 \\
sX_2 &= aX_1 - (b+d)X_2 + eX_3 \\
sX_3 &= bX_2 - (c+e+g)X_3 + fX_4 \\
sX_4 &= cX_3 - (f+h)X_4 \\
sX_5 &= gX_3 + hX_4
\end{aligned}$$

with initial conditions, $x_1(0) = 1$, $x_2(0) = x_3(0) = x_4(0) = x_5(0) = 0$. $X_1$, $X_2$, $X_3$, $X_4$, and $X_5$ denote the Laplace transforms of $x_1$, $x_2$, $x_3$, $x_4$, and $x_5$, respectively, and s denotes the Laplace operator.

Figure 3.4-2 shows the mean failure rate (MFR) (see appendix A), for a range of values of $1-p_1$ and f. The parameters $p_2$ and ds were fixed at the values $p_2 = 0$ and ds = 10/hour. Sensitivity studies indicate that the MFR is insensitive to values of ds between 1 and 10 per hour.

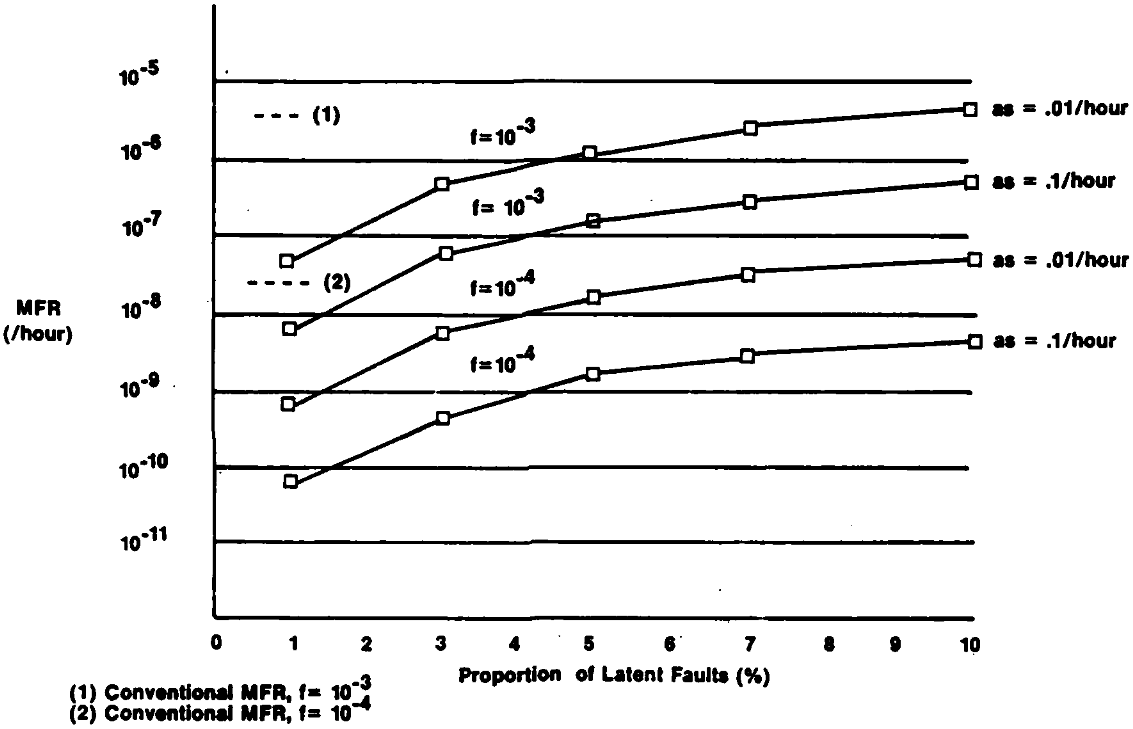


FIGURE 3.4-2. MEAN FAILURE RATE/TRIPLEX FCS

These results are summarized in tables 3.4-1 and 3.4-2 for lane failure rates ($10^{-3}$/hour and $10^{-4}$/hour, respectively). It is noted that the corresponding MFRs, based on conventional reliability analysis, are $3\text{x}10^{-6}$/hour and $3\text{x}10^{-8}$/hour, respectively.

TABLE 3.4-1. MFR, TRIPLEX FCS, $f = 10^{-3}$/HOUR

| as(/hour) | $1-p_1$(%) | MFR(/hour) |
|---|---|---|
| .1 | 10 | $5.76\text{x}10^{-7}$ |
| .1 | 7 | $2.82\text{x}10^{-7}$ |
| .1 | 5 | $1.44\text{x}10^{-7}$ |
| .1 | 3 | $5.19\text{x}10^{-8}$ |
| .1 | 1 | $5.77\text{x}10^{-9}$ |
| .01 | 10 | $4.47\text{x}10^{-6}$ |
| .01 | 7 | $2.20\text{x}10^{-6}$ |
| .01 | 5 | $1.13\text{x}10^{-6}$ |
| .01 | 3 | $4.07\text{x}10^{-7}$ |
| .01 | 1 | $4.53\text{x}10^{-8}$ |

TABLE 3.4-2. MFR, TRIPLEX FCS, $f = 10^{-4}$/HOUR

| as(/hour) | $1-p_1$(%) | MFR(/hour) |
|---|---|---|
| .1 | 10 | $5.92\text{x}10^{-9}$ |
| .1 | 7 | $2.90\text{x}10^{-9}$ |
| .1 | 5 | $1.48\text{x}10^{-9}$ |
| .1 | 3 | $5.33\text{x}10^{-10}$ |
| .1 | 1 | $5.92\text{x}10^{-11}$ |
| .01 | 10 | $5.81\text{x}10^{-8}$ |
| .01 | 7 | $2.85\text{x}10^{-8}$ |
| .01 | 5 | $1.45\text{x}10^{-8}$ |
| .01 | 3 | $5.23\text{x}10^{-9}$ |
| .01 | 1 | $5.82\text{x}10^{-10}$ |

### 3.4.1. Mean Failure Rate Approximation

An approximate value of MFR can be obtained as follows:

On the average, loss of control will occur if two latent faults occur in a time interval of length 1/as hours and no $\alpha$-faults occur in either of the lanes containing the latent faults. If q denotes this prɔbability, then

$$\begin{aligned} q &\approx 6[(1-p_1)f/as]^2[1 - 2(p_1)f/as] \\ &\approx 6(1-p_1)^2f^2(1/as)^2 \end{aligned} \qquad (1)$$

Thus, the Mean Time to Failure (MTTF) is:

$$\begin{aligned} \text{MTTF} &\approx (1/as)[\ q + 2(1-q)q + 3(1-q)^2q + \dots\ ] \\ &= (1/as)/q \end{aligned} \qquad (2)$$

$$\begin{aligned} \text{MFR} &\approx q(as) \\ &\approx 6(1-p_1)^2f^2/as \end{aligned} \qquad (3)$$

### 3.4.2. Summary of Example 1

- The relative effect of latent faults is conveniently described by the ratio

  $$R = \frac{\text{probability of loss of control with latent faults}}{\text{probability of loss of control by conventional analysis}}$$

  For values of $R << 1$, the effects of latent faults are insignificant. From the tables, the maximum value of R is .97 (for $f = 10^{-4}$, $as = .01$, $p_1 = .9$).

- Relative to the conventional MFR, a Triplex FCS does not appear to be especially vulnerable to latent faults; in the worst case, survivability is reduced by a factor of two.

- MFR is directly proportional to $(1-p_1)^2$.

- MFR is directly proportional to 1/as, the "time on risk."

- Survivability is adversely affected by the proportion of latent faults, $1 - p_1$, although for the range of parameters selected, this effect is not significant.

### 3.5. Example 2 - Quadruplex FCS

The conventional reliability analysis would indicate that probability of loss of the FCS function in a flight of one hour $= 4f^3$.

A Markov reliability model of the FCS is shown in figure 3.5-1. The assumptions are the same as for the triplex system.

Referring to figure 3.5-1:

- State $S_1$ represents the condition that all lanes are fault-free.

- State $S_2$ has a latent fault in one lane.

- State $S_3$ has a latent fault in two lanes.

- State $S_4$ has a latent fault in three lanes.

- State $S_5$ has a latent fault in four lanes.

- State $S_6$ represents loss of the FCS function.

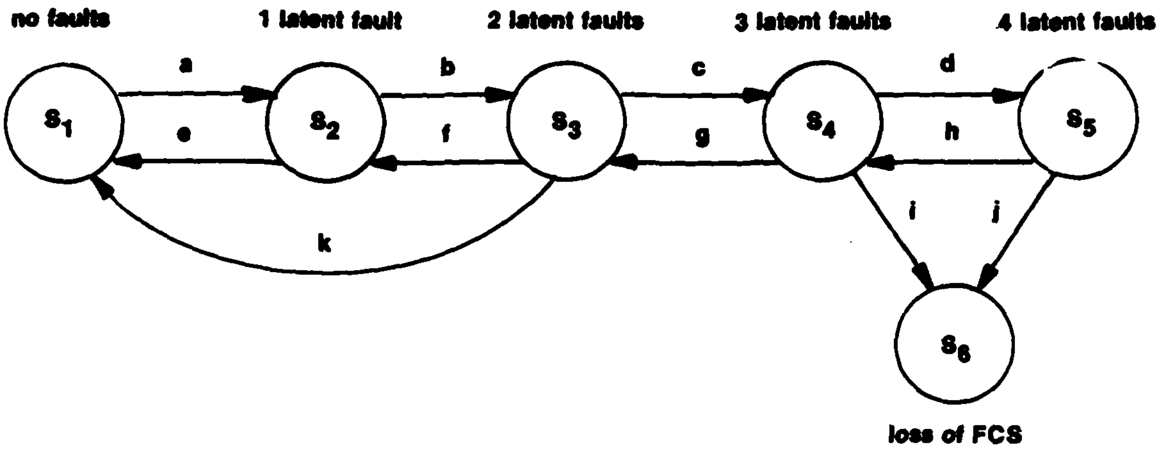


FIGURE 3.5-1. MARKOV MODEL/QUADRUPLEX FCS WITH LATENT FAULTS

The transition rates are:

$$a = 4(1-p_1)f\left[\frac{ds}{as + ds}\right]$$

$$b = 3(1-p_1)f$$

$$c = 2(1-p_1)f$$

$$d = (1-p_1)f$$

$$e = as + (p_1)f$$

$$f = 2(p_1)f$$

$$g = 3(p_1)f$$

$$h = 4(p_1)f$$

$$i = as$$

$$j = as$$

$$k = as$$

Again, it is noted that the backward transitions (e, f, g, h, and k) are the result of repairs due to the detection of α-faults.

From the figure we obtain the following differential equations:

$$
\begin{aligned}
sX_1 - x_1(0) &= -aX_1 + eX_2 + kX_3 \\
sX_2 &= aX_1 - (b + e)X_2 + fX_3 \\
sX_3 &= bX_2 - (c + f + k)X_3 + gX_4 \\
sX_4 &= cX_3 - (d + g + i)X_4 + hX_5 \\
sX_5 &= dX_4 - (h + j)X_5 \\
sX_6 &= iX_4 + jX_5
\end{aligned}
$$

with initial conditions, $x_1(0) = 1$, $x_2(0) = x_3(0) = x_4(0) = x_5(0) = x_6(0) = 0$. $X_1$, $X_2$, $X_3$, $X_4$, $X_5$, and $X_6$ denote the Laplace transforms of $x_1$, $x_2$, $x_3$, $x_4$, $x_5$, and $x_6$, respectively.

Figure 3.5-2 shows the MFR for a range of $1-p_1$ and f with $p_2$ and ds again fixed at $p_2 = 0$, ds = 10/hour. These results are summarized in tables 3.5-1 and 3.5-2 for lane failure rates, $10^{-3}$/hour and $10^{-4}$/hour, respectively.

It is noted that the corresponding MFRs, based on conventional reliability analysis, are $4x10^{-9}$/hour and $4x10^{-12}$/hour, respectively.

TABLE 3.5-1. MFR, QUADRUPLEX FCS, F = $10^{-3}$/HOUR

| as(/hour) | $1-p_1$(%) | MFR(/hour) |
|---|---|---|
| .1 | 10 | $2.23x10^{-9}$ |
| .1 | 5 | $2.80x10^{-10}$ |
| .1 | 3 | $6.04x10^{-11}$ |
| .1 | 1 | $2.24x10^{-12}$ |
| .01 | 10 | $1.37x10^{-7}$ |
| .01 | 5 | $1.73x10^{-8}$ |
| .01 | 3 | $3.75x10^{-9}$ |
| .01 | 1 | $1.39x10^{-10}$ |